

**Workshop on Security Procedures for the
Interchange of Electronic Documents**

National Institute of Standards and Technology
Gaithersburg, Maryland
November 12-13, 1992

**LINKING SECURITY AND
THE LAW OF COMPUTER-BASED COMMERCE**

by

Michael S. Baum, J.D., M.B.A.
Independent Monitoring
Cambridge, Massachusetts USA
Now of VeriSign
Mountain View, CA

PREFACE

It is frequently (and astutely) stated that the law has not kept pace with technology. The historical tensions of law reform intended to accommodate technological change are manifested in the words of Oliver Wendell Holmes, who said

[a]s few could write, most people had to authenticate a document in some other way, for instance, by making their mark. This was, in fact, the universal practice in England until the introduction of Norman customs. With them seals came in. But as late as Henry II they were said by the Chief Justice of England to belong only to kings and to very great men. I know no ground for thinking that an authentic charter had any less effect at that time when not under seal than when it was sealed. . . . Its conclusive effect was due to the satisfactory nature of the evidence, not to the seal. . . . But when seals came into use they obviously made the evidence of the charter better, in so far as the seal was more difficult to forge than a stroke of the pen.¹

Similarly, the Supreme Court stated that

[f]ormerly wax was the most convenient, and the only material used to receive and retain the impression of a seal. . . . We cannot perceive why paper, if it have that capacity, would not as well be included in the category. The simple and powerful machine, now used to impress public seals, does not require any soft or adhesive substance to receive or retain their impression. The impression made by such a power on paper is as well defined, as durable, and less likely to be destroyed or defaced by vermin, accident, or intention than that made on wax. It is the seal which authenticates, and not the substance on which it is impressed; and where the court can recognize its identity, they should not be called upon to analyze the material which exhibits it.²

Just as prior generations have grappled with document trustworthiness, today we must creatively forge a path which accommodates current requirements and practices, while contemplating the future. *Solutions* necessarily require compromises -- the challenge is to develop solutions and compromises

¹ OLIVER WENDELL HOLMES, THE COMMON LAW 272-273 (1881).

² *Pillow v. Roberts*, 54 U.S. (13 How.) 472, 473-74 (1851).

that are thoughtful, practical and extensible. This is a daunting undertaking, but it is, at the same time, necessary and exciting.

TABLE OF CONTENTS

I. Introduction	1
II. Security and Reliability	3
a. Treatment in the Law	3
b. Reasonable Security Procedures	12
c. Mapping Security Attributes to Legal Standards	16
Table 1 - Comparison of Signed Writings and Electronic Information*	17
Table 2 - Fallibilities of Paper-based Signatures	18
d. Non-repudiation	19
e. Trusted Entities and Time Stamping	21
III. Risk Analysis and Risk-Based Approaches.....	23
a. Risk Analysis	23
b. Security Baseline Issues	25
Table 3 - Relative Levels of Abstraction.....	26
Table 4 - Survey of Costs in Implementing Cryptography.....	33
Table 5 - Primary Beneficiary of Security	35
c. A Model Security Baseline	35
IV. Burden of Proof and Presumptions.....	44
Table 6 - Substitute Model Baseline Section 3 - Legal effect	51
V. Integrating Formalistic & Evidentiary Requirements.....	52
Figure 1 - A Hypothetical Cradle-to-Grave Transaction	53
Table 7 - Effect of Differing Formalistic & Foundational Requirements	55
VI. Conclusion	56
Appendix - The Model Security Baseline Graphics	57

ACKNOWLEDGMENTS

The author gratefully acknowledges the comments and suggestions of many people, and particularly the significant comments and suggestions of the following people: Thomas Armstrong, Esq., U.S. General Accounting Office; George Chandler, Esq., Hill, Rivkin, Lomberg, O'Brien, Mulroy & Hayden; Douglas S. Cohen, Boston University Law School; Jerry Cohen, Esq., Perkins, Smith & Cohen; Clyde Christofferson, Esq.; Richard Dodd, Esq.; Sandy Epstein, Racal-Guardata, Inc.; Robert Fougner, Esq., PKP; Françoise Gilbert, Esq.; Altheimer & Gray; Gregory A. Gilbert, Boston University Law School; Ted Humphreys, XISEC Consultants Ltd.; Claire Johnson, Esq., Wilde Sapte; Gregory P. Joseph, Esq., Fried, Frank, *et al.*; Steve Kent, Ph.D., BBN; Professor Emeritus Alfred I. Maleson, Suffolk University Law School; Jerry Rainville, Esq., NSA; Miles Smid, NIST; Thomas Smedinghoff, Esq., McBride, Baker & Coles; Lee Stanton, General Electric Information Services; Oliver Smoot, Esq., CBEMA; and Peter Weiss, Esq., OMB.

AUTHORSHIP

Michael S. Baum is Principal of Independent Monitoring, a Cambridge, Massachusetts consultancy specializing in electronic data interchange and electronic commerce law and security. Baum chairs the EDI and Information Technology Division and the Information Security Committee, Section of Science and Technology, American Bar Association. The views expressed in this article do not necessarily reflect those of any organization or person other than the author. Because this paper presents some new or otherwise untested ideas, and because the subject matter of this paper begs further debate and consideration, comments and criticism are respectfully solicited.

Michael S. Baum
33 Tremont Street
Cambridge, MA 02139-1227 USA
FON: 1-617-661-1234
FAX: 1-617-661-0716
INTERNET: baum@hulaw1.harvard.edu

New Address
1390 Shorebird Way
Mountain View, CA 94043
TEL. 1-650-429-3444
FAX. 1-650-429-5113
INTERNET: michael@verisign.com

LINKING SECURITY AND THE LAW OF COMPUTER-BASED COMMERCE

by

Michael S. Baum, J.D., M.B.A.

I. INTRODUCTION

The accelerating movement from paper-based transactions and records to their electronic replacements, and the resulting benefits from this movement, are well documented. Yet in many cases, the shift from conventional to electronic mechanisms has not enjoyed sufficient legal consideration and treatment. Real and *perceived*³ security weaknesses of electronic transactions and records remain legal and practical barriers to their effective widespread use. This paper considers the legal efficacy⁴ and expanded use of electronic transactions and records in

³ Arguably, perceived security weaknesses could be reduced or eliminated by accepting commercially reasonable security practices (*see infra*). The failure to do so causes perceived weaknesses to become unnecessary barriers.

⁴ *Legal efficacy* in this paper denotes wide legislative and judicial recognition that properly secured electronic transactions and records satisfy traditional legal indicia of reliability. These indicia include, where appropriate, transactions or communications considered to be *in writing, signed, verified, or acknowledged*. Such legal requirements often differ considerably among states and among nations, as well as by application. Some attributes of conventional paper-based media are difficult to reproduce by electronic media, such as their singularity (uniqueness), which is an attribute of critical importance to negotiable instruments and comparable legal instruments. *See infra* TABLE 1 (distinguishing various security attributes, including singularity), and Section II.e. TRUSTED ENTITIES AND TIME STAMPING (noting that electronic "trusted entities" can assure the requisite singularity).

This paper neither endorses nor condemns *writing, signing*, or other requirements that historically support conventional paper-based attestations and commitments. Legal analysis of these requirements and responsive private and legislative reform should consider and reflect pragmatically the underlying attributes and objectives of such requirements (*e.g.*, authentication and integrity). A mere redefinition of *writing* and *signature* is not recommended.

modern commerce, government, and other environments for undertaking commitments and other important purposes. The paper also asserts that information security mechanisms exist, considers their associated costs and benefits, and advocates, where appropriate, the use of such mechanisms. A model security baseline is proposed. The goal is to arrive at a reasonable level of security for various classes of transactions and records to provide assurances of satisfying legal requirements. The thrust of this paper, however, focuses on the legal implications of authentication, integrity, non-repudiation and availability rather than on those of confidentiality.⁵ This focus is not intended, however, to underplay the criticality of responsive private and government treatment of confidentiality issues -- indeed, confidentiality is the most critical requirement in some applications.⁶ While this paper presents some "action-oriented" proposals, clearly the work has only begun.

⁵ These five important security services are commonly defined as follows:

Authentication - The corroboration that the source of data received is as claimed; or the establishment or verification of a claimed identity (1) to verify the identity of a user, device, or other entity in a computer system and (2) to verify the integrity of data that have been stored, transmitted, or otherwise exposed to possible unauthorized modification. Cf., FED. R. EVID. 901(a) Requirement of Authentication or Identification, General Provision, "[T]he requirement of authentication . . . is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims."

Integrity - The property that data has not been altered or destroyed in an unauthorized manner; Sound, unimpaired or perfect condition.

Non-repudiation - *see infra* text to note 67.

Availability - The property of being accessible and usable upon demand by an authorized entity.

Confidentiality - The property that information is not made available or disclosed to unauthorized individuals, entities, or processes. The concept of holding sensitive data in confidence, limited to an appropriate set of individuals or organizations.

These definitions are taken from International Standards Organization 7498-2-1988(E) ("ISO"); and the National Computer Security Center, Glossary of Computer Security Terms, NCSC-TG-004 Version 1 (Oct. 21, 1988) ("Glossary"). Note, non-repudiation is not defined in the Glossary.

⁶ See, e.g., WORKGROUP FOR ELECTRONIC DATA INTERCHANGE (WEDI), REPORT TO SECRETARY OF U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES, Recommendation 8 (relating to confidentiality -- the WEDI recommendations did not include a comparable recommendation on information authenticity and integrity) (July 1992). "Confidentiality provision is considered by most users as less immediately important. In the future, however, this situation is likely to change as advanced communication services . . . will become all-pervasive." Action Line 3.3., Official Jour. of the European Commission, No. L 123/23 (May 8, 1992) (hereinafter "E.C.").

II. SECURITY AND RELIABILITY

a. Treatment in the Law

The creation, processing, communication, control, management, storage, use, retention, and retrieval of information in electronic form⁷ have become critical to modern society. However, Electronic Data Interchange ("EDI")⁸ and transactions and records in electronic form are not yet accorded the extent of the legal efficacy enjoyed by paper-based transactions and records. Before these electronic forms can earn this legal efficacy, they must establish customs and practices, or they must at least be judged legally equivalent to their manual counterparts.⁹ This problem of legal efficacy arises in the following areas of law,

⁷ Hereinafter, references to *records* or *information in electronic form* will include their electronic creation, processing, communication, control, management, storage, use, retention and retrieval unless expressly qualified. *See infra* FIGURE 1 - A HYPOTHETICAL CRADLE-TO-GRAVE TRANSACTION (demonstrating a hypothetical transaction process for information in electronic form).

⁸ EDI is the exchange, between organizational entities, of computer processable data in a standard format. For example, the information contained in a conventional purchase order, invoice or health care payment claim can be communicated in electronic form such that the recipient's computer system can process the data meaningfully without human intervention. *See generally* DATA INTERCHANGE STANDARDS ASSOCIATION, INTRODUCTION TO ELECTRONIC DATA INTERCHANGE (1990); FIPS-PUB 161 (discussing EDI). This paper also uses the familiar term "electronic commerce," which is recognized as a subset of EDI. The term "computer-based commerce" is proffered as more generic than *electronic* commerce -- recognizing that use of optical and future unknown technologies must be accommodated.

⁹ EDI technical and security standards do not serve as a substitute for responsive legal consideration. Such standards are purposefully drafted to provide options and alternatives to accommodate use by diverse industries and do not necessarily provide the guidance necessary to assure the creation of unequivocal legal acts. Technical standards developers cannot properly analyze and resolve complex legal issues. As noted by the United Nations Commission on International Trade Law (UNCITRAL), legislation, when specifically permitting or requiring authentication to be made by EDI, *should require evidence of conformity with an applicable EDI protocol*, at least as a condition of attracting a presumption of authenticity, the onus of proof being shifted to the party asserting the authenticity of the message in cases where the requirement of the protocol are not satisfied." *ELECTRONIC DATA INTERCHANGE -- PRELIMINARY STUDY OF THE LEGAL ISSUES RELATING TO THE FORMATION OF CONTRACTS BY ELECTRONIC MEANS*, 23 U.N. GAOR CN.9 at 15, U.N.

among others: contracts, evidence, government procurement and regulation, criminal law, real property, and the judicial process.

1. Contracts -- Seeking to satisfy requirements for electronic transactions and records under the Uniform Commercial Code ("U.C.C."), raises certain fundamental issues.¹⁰ For example, although the definition of *signed* in U.C.C. § 1-201(39) "includes any symbol executed or adopted by a party with the present intention to *authenticate* a writing" (emphasis added), the word *authenticate* is not defined in U.C.C. Articles 1 or 2 (although Official Comment 39 to U.C.C. § 1-201 includes mention of a thumbprint (a particularly forensically-intensive¹¹ type of authentication). This lack of definition has created confusion in the legal community. While the case law considering electronic writings and signatures is sparse and inconsistent, some of those cases addressing the issue confirm the importance of the probative value of signatures.¹²
2. Evidence -- The Federal Rules of Evidence do not address specifically electronic digital data security mechanisms.¹³ The scope of proof of trustworthiness (and, arguably, security) as an evidentiary foundation

Doc. A/CN.9/333 (1990) (hereinafter "UNCITRAL Study") (emphasis added); *see also* 1991 UNCITRAL ¶ 66. *See infra* Section IV. BURDEN OF PROOF AND PRESUMPTIONS.

- ¹⁰ *See, e.g.*, U.C.C. § 2-201 (Statute of Frauds); U.C.C. § 1-201(39) (defining "signed") and U.C.C. § 5-104 (addressing Formal Requirements and Signing).
- ¹¹ *See generally*, BAUM, EDI AND THE LAW (Walden, ed. 1989) § 9.4 "The signing Requirement" at 123-125 (asserting that signatures and their electronic analogs should carry "forensic characteristics providing probative evidence of identity").
- ¹² *See In re Carlstrom*, 3 U.C.C. Rep.Serv. 766, 773 (Bankr. D.Me. 1966) (requiring the affixed symbol for signature purposes under U.C.C. § 9-402 (Formal Requisites of Financing) to be *susceptible of evidentiary connection to the signatory*). "If we content ourselves with any symbol as a sufficient signature regardless of its evidentiary worth, not only must the legislative design of enhancing the authenticity of the public record fail, but in addition, there will have been erected a purely formalistic and purposeless pitfall for bona fide lienors." *id.* *See also In re Brawn Coca-Cola Bottling Plants, Inc. v. Tabenken*, 7 U.C.C. Rep.Serv. 565 (Bankr. D.Me. 1970).
- ¹³ *Cf.* FED. R. EVID. 901(b)(9) (Process or system), 1001(1) (Writings and recordings), 1001(3) (Original), 902 (Self-Authentication), and N.J. R. EVID. 1(13) (writing); *see Peritz, Computer Data and Reliability*, 80 Nw. U.L. Rev. 956 (1986) *reprinted in* 7 Comp. L.J. 23 (1986). *See Transport Indemnity Co. v. Seib*, 132 N.W.2d 871 (Neb. 1965) (noting that taped record prepared by computer for purposes of trial are not precluded under the Business Records Act).

requires closer scrutiny. "[B]ecause electronic files are particularly susceptible to purposeful or accidental alteration, or incorrect processing, laying a foundation for their admission must be done with particular care. Proper control over creation and maintenance of these files can be crucial in overcoming inevitable objections that will be raised in the courtroom."¹⁴ The implications of burgeoning, open, interconnected, and highly diverse computer systems utilizing expert system components, which may change frequently and considerably, may call for strong evidentiary foundations.¹⁵

There is some case law supporting the notion that proof of reliability (and implicitly security) is recognized as appropriate and necessary in evaluating the admissibility of computer-based evidence.¹⁶ Other cases suggest a relaxation of the foundation required for admissibility of certain computer-based information (absent abuse of discretion by the judge).¹⁷

¹⁴ U.S. DEPT. OF JUSTICE, *ADMISSIBILITY OF ELECTRONICALLY FILED FEDERAL RECORDS AS EVIDENCE: A GUIDELINE FOR FEDERAL MANAGERS AND COUNSEL* (Oct. 1990) at 2. "The increasing use of computers in creating and managing records in the ordinary course of business has resulted in the courts' tending to treat printouts of electronically stored 'business' records no differently than other records. However, the increased complexity of safeguarding the integrity of computer files accessible through remote terminals can dampen this tendency. In any event, computer records not offered as business records will continue to present special foundation problems often requiring the testimony of technical experts." *id.* at 17. "The effectiveness and reliability of each party's security procedures. . . may be relevant in individual cases to the ultimate admissibility of any Signed [electronic] Documents." A MODEL EDI TRADING PARTNER AGREEMENT § 3.3 Comment 7, 45 Bus. Law. 1717 (1990).

¹⁵ See Section V. INTEGRATING FORMALISTIC AND EVIDENTIARY REQUIREMENTS, *infra* (examining evidentiary requirements for the laying of a foundation).

¹⁶ See *U.S. v. Scholle*, 553 F.2d 1109, 1124-25 (8th Cir.), *cert. denied*, 434 U.S. 940 (1977) (stating that computer storage needs a more comprehensive foundation for admissibility, including testimony on procedures for input control, such as a test for insuring accuracy and reliability); *U.S. v. Russo*, 480 F.2d 1228, 1239-44 (6th Cir. 1973) (holding that authentication of computer records requires establishing reliability and trustworthiness of information put into computer).

¹⁷ See, e.g., *Rosenburg v. Collins*, 624 F.2d 659 (5th Cir. 1980); *U.S. v. Vela*, 673 F.2d 86, *reh'g den.* 677 F.2d 113 (5th Cir. 1982), and *U.S. v. Linn*, 880 F.2d 209 (9th Cir. 1989). Note, however, that each of these cases involved telephone company billing records -- records which are created and retained by *trusted third parties*. For a further discussion of trust entities, see *infra* Section II.e. TRUSTED ENTITIES AND TIME STAMPING. In *U.S. v. Weatherspoon*, 481 F.2d 595, 598 (7th Cir. 1978) a college's falsified student enrollment

The Manual for Complex Litigation Second (1985) recognizes and addresses this problem of proof of reliability, yet by focusing on weight rather than admissibility, it reaches an equivocal, and ultimately unsatisfactory, solution of such evidentiary issues. It observes that "[n]otwithstanding the capacity of computers to make tabulations and calculations involving enormous quantities of information . . . several sources of potential errors of great magnitude exist."¹⁸ The Manual further notes that the proponent of computerized evidence has the burden of laying a proper foundation by establishing its accuracy,¹⁹ and "the existence or possibility of errors usually affects only the weight, not the admissibility of the evidence, except when the problems are so significant as to call for exclusion . . ."²⁰

3. Government Procurement and Regulation -- Interpretation and resolution of State, Federal and foreign requirements such as those concerning signature requirements remains unsettled. Compare the following varied -- arguably conflicting -- signature definitions.

cards where used to defraud the Veteran's Administration. The court determined that the following foundation was sufficient for admissibility of computer printouts by the VA supervisory employee familiar with printouts: "(1) what the input procedures were, (2) that the input procedures and printouts were accurate within two percent, (3) that the computer was tested for internal programming errors on a monthly basis, and (4) that the printouts were made, maintained and relied on by the VA in the ordinary course of business activities."

¹⁸ MANUAL FOR COMPLEX LITIGATION SECOND § 21.446 (1985).

¹⁹ *Id.*

²⁰ *See supra* note 81. "In view of the complex nature of the operation of computers and general lay unfamiliarity with their operation, courts have been cautioned to take special care to be certain that the foundation is sufficient to warrant a finding of trustworthiness and that the opposing party has full opportunity to inquire into the process by which information is fed into the computer." MCCORMICK, HANDBOOK OF THE LAW OF EVIDENCE, (2d Ed. 1972) at 734. *See also* American Oil Co. v. Valenti, 426 A.2d 305, 310 (CT 1979) (recognizing that "[b]usiness records that are generated by computers present structural questions of reliability that transcend the reliability of the underlying information that is entered into the computer" due to both hardware and software errors.); *but see* U.S. v. Hutson, 821 F.2d 1015, 1020 (5th Cir. 1987) ("The district court is given great latitude on the issue of trustworthiness.").

- i. *signature* - "includes a mark when the person making the same intended it as such"²¹;
- ii. *signed* - "includes any symbol executed or adopted by a party with the present intention to authenticate a writing"²²;
- iii. *signed* - "shall include the entry in the form of a magnetic impulse or other form of computer data compilation of any symbol or series of symbols executed, adopted or authorized as a signature"²³;
- iv. *signature* - "in the case of an EDI transmission, means a discrete authenticating code intended to bind parties to the terms and conditions of a contract"²⁴; and
- v. *electronic signatures* - "characters representing the nominated persons on documents, and signed or symbols identifying their writers."²⁵

One working group which considered this issue apprehended the effect of such uncertainty when it concluded that "[t]he lack of adoption of an accepted electronic signature policy by the [Department of Defense] will prevent some contract transactions being conducted in digital form."²⁶ Independently, the Comptroller General has addressed uncertainty in electronic commerce with the following decision: "[c]ontracts formed using Electronic Data Interchange technologies may constitute valid obligations of the government for purposes of 31 U.S.C. § 1501, so long as the technology used provides the same degree of assurance and certainty as traditional 'paper and ink' methods of contract formation."²⁷ Nevertheless, outside of

²¹ 1 U.S.C. § 1.

²² U.C.C. § 1-201(39).

²³ 17 C.F.R. § 230 (1990).

²⁴ 41 C.F.R. § 101-41.002(d) (1990).

²⁵ Korean Act on Promotion of Trade Business Automation (1992) (Law No. 4479 Enacted Dec. 31, 1991) Art. 2.8 (Definitions, "Electronic Signature") reprinted in UN/ECE/TRADE/WP.4/R.872 (Aug. 4, 1992) (hereinafter "Korean Act") at 5.

²⁶ Legal Issues Committee of the Acquisition Task Group, CALS/EC Industry Steering Group, Report on Potential Legal Issues Arising from the Implementation of CALS by the DoD (Nov. 10, 1991) at 10.

²⁷ Matter of National Institute of Standards and Technology--Use of Electronic Data Interchange Technology to Create Valid Obligations, Dec. of the Comp. Gen. of the U.S.,

the specific circumstances presented in the NIST case, the decision begs for a closer definition of the indicia of assurance and certainty necessary to be deemed reliable.

4. Real Property -- An example of how the problem of legal efficacy of electronic information could arise in the real property area involves the recording of deeds and related instruments where the recording statute mandates that "writings which are to be recorded or docketed in the clerk's office of courts of record in this Commonwealth shall be an original or first generation printed form, or legible copy thereof, pen and ink or typed ribbon copy. . . ." ²⁸ Such a statute raises considerable barriers to computer-based commerce.
5. In Relation to the Judicial Processes -- The legal efficacy of information in electronic form also arises in judicial contexts. Despite the advance of computer automation in some aspects of the judicial process, electronic notice and service of process are not generally permitted by court rules. However, there are exceptions, ²⁹ and judicial reform is accelerating. ³⁰

File B-245714 (Dec. 13, 1991). This opinion arose from a request by National Institute of Standards and Technology (hereinafter "NIST") to determine "whether agencies can use Electronic Data Interchange (EDI) technologies to create valid contractual obligations that can be recorded consistent with 31 U.S.C. § 1501." See TABLE 2 - FALLIBILITIES OF PAPER-BASED SIGNATURES, *infra* Section.II.c.

²⁸ VA. CODE § 55-108.

²⁹ E.g., FED. R. APP. P. 25(a) (1991) (authorizing a court of appeals to accept papers filed "by facsimile or other electronic means"); OHIO R. C. P. Rules 5(e) and 10 (July 1, 1991). The National Archive and Records Administration's *Electronic Records Management* regulations accommodate the judicial use of electronic records pursuant to FED. R. EVID. 803(8). 36 C.F.R. § 1234.24 (1990).

³⁰ Additionally, the U.S. Department of Justice has issued findings which "encourage the development of electronic data interchange technologies." BUREAU OF JUSTICE STATISTICS, REPORT OF THE NATIONAL TASK FORCE ON CRIMINAL HISTORY RECORD DISPOSITION REPORTING, NCJ-135836 (June 1992) at 1. Also, efforts to incorporate EDI into the judicial process have been undertaken both domestically -- by the Administrative Office of the U.S. Courts, the National Center for State Courts, the Judicial EDI Consortium -- and abroad -- by the French Ministry of Justice, EDIFRANCE and the Association pour le développement de l'informatique juridique.

It is evident from the above discussion of the different legal fields that there is need for legal reform. As noted in the *Uniform Rules of Conduct for Interchange of Trade Data by Teletransmission* ("UNCID"), a pioneering international code of conduct that addresses important legal and control considerations attendant to the use of electronic trade data, the

electronic document is quite different [from a paper document]. It takes the form of a magnetic medium whose data content can be changed at any time. Changes or additions will not appear as such it is possible to establish techniques which give electronic data interchange characteristics that make it equal or superior to paper not only as [a] carrier of information, but also as regards the evidential functions.³¹

Moreover, electronic transactions are increasingly communicated within open, distributed and interconnected environments.³² These environments potentially expose users and networks to risks from both accidental and deliberate alteration and destruction of data,³³ because open environments are generally more difficult to control than are closed ones.³⁴ "New vulnerabilities

³¹ INTERNATIONAL CHAMBER OF COMMERCE, Pub. No. 452 (1988) at 8. UNCID further states that "[f]irstly EDI in itself presupposes procedures that make this form of communication more secure. In addition to identification this technique can also provide for error detection and correction. Authentication in the sense that the data content is correct can also be established." *Id.* It is anticipated that guidelines for the security of information systems concerning a broad spectrum of information security issues will soon be submitted to the Organisation for Economic Co-operation and Development (O.E.C.D.) Council for adoption.

³² See generally, NATIONAL RESEARCH COUNCIL, COMPUTERS AT RISK, SAFE COMPUTING IN THE INFORMATION AGE (1991) (hereafter "NRC"). "[T]he risk of bad data seriously harming your business increases as your organization moves from a series of isolated databases to massive, distributed databases that all employees can access. 'We're seeing just the tip of the iceberg'." *Devil In Your Data*, INFORMATIONWEEK (Aug. 31, 1992) at 48.

³³ See Eckerson, *Network security lacking at major stock exchanges*, Network World (Sept. 16, 1991) at 23-24; Prefatory Note, U.C.C. Art. 4A (1990); see also *Shell Pipeline v. Coastal States Trading*, 788 S.W. 2d 837 (Tex. Ct. App. 1990) (Shell's responsibility for correction of errors was upheld, even where Shell's undertaking [which paralleled some third party services] was "entirely gratuitous").

³⁴ Because conventional management techniques and controls cannot respond adequately to open and distributed environments, technology-based techniques and controls may be necessary. Notwithstanding, this neither suggest nor implies that conventional security and management techniques (including physical security, internal controls and audit trails, including message acknowledgments) are other than indispensable.

are emerging as computers become more common as components of domestic and international financial systems. *The nation needs computer technology that supports substantially increased safety, reliability, and, in particular, security.*"³⁵

Additionally, in open environments, parties will increasingly desire or need to communicate and make commitments without having executed electronic trade and communication agreements. Consequently, the degree of *end-to-end* security³⁶ in such trading environments takes on increased importance.³⁷ "[I]f the

³⁵ NRC, *supra* note 32 at 2 (emphasis by Council). This view is substantiated by reports of increasing problems. For example, "[i]t [was] estimated that security breaches, including lost revenue, data recovery, lost computing time, and personal downtime . . . cost U.S. corporations \$1 billion in 1990." YANKEE GROUP, DATA NETWORK RELIABILITY AND SECURITY (1990); *Facing Up to Liability*, INFORMATIONWEEK (Sept. 7, 1992) at 58 ("[t]otal cost of toll fraud targeted at user-owned systems \$2.2 billion"); FINDINGS OF THE GEN. ASSEMBLY OF THE STATE OF GEORGIA, GEORGIA COMPUTER SYSTEMS PROTECTION ACT (Code 1981, § 16-9-90, enacted by Ga. L. 1991, ¶ 1045, § 1) ("[t]he opportunities for computer related crimes in state programs, and in other entities which operate within the state, through the introduction of fraudulent records into computer systems, unauthorized use of computer facilities, alteration or destruction of computerized information files, and stealing of financial instruments, data, or other assets are great."). See Bigelow, "Computer Security, Crime and Privacy in the USA -- A Status Report," COMP. LAW AND SEC. REP., Vol. 8, Issue 4 (Jul.-Aug. 1992) at 146-154 (includes a useful list of additional attacks, threats and caveats relative to information security); Barton Crockett, "ACH Payment System Seen Vulnerable to Fraud Losses," American Banker (Jul. 29, 1992) at 5 (noting loss of nearly \$70 million by First Interstate Bank of California due to apparently fraudulent transaction instructions). "Discussion indicated broad recognition that EFT is highly vulnerable to illicit exploitation unless adequate security measures are employed." Treasury Directive 81-80, § 2.1.

³⁶ End-to-end security refers to those sets of services that are applied to information prior to their submission to the communication mechanism. These services provide security assurances throughout the transfer to the intended recipient and which are verifiable by the recipient. Such services may include, but are not limited to, digital signatures for authenticity and integrity, and encryption for privacy purposes. Note, Treasury Directive 81-80 "implicitly recogniz[es] that voluntary adoption of end-to-end authentication is, in the long run, far preferable." § 2.3. "The existence of end-to-end security service without some prior arrangement is a security oxymoron . . . without a secure start-up with some locust of trust, there is no security." Letter from Jerry Rainville, Esq., NSA to Michael S. Baum (Nov. 5, 1992) (on file with author).

³⁷ The U.S. Department of Defense has recognized the weaknesses in such open communications environments: "[i]t is important to reiterate that the CN [communication network] is not relied upon for the confidentiality or integrity of the information it transfers. Failures in a CN can only result in the delay, mis-delivery, or non-delivery of otherwise adequately protected information." Draft DOD INFORMATION SYSTEMS

information is shared between user groups or exchanged via a public or generally accessible [] network . . . [n]either the technology, terminals and services nor the related standards and procedures are generally available to provide comparable security for information systems in these cases."³⁸

Although the extent (or strength) of the security necessary to support reliable electronic transactions and records for legal purposes is unclear, security is increasingly recognized as critical.³⁹ This conclusion is supported by decisions,

SECURITY POLICY at § 4.4 "FIRST PROTECTION ALLOCATIONS" (March 30, 1992) (note: this is not yet DoD policy).

The extent to which we should trust networks becomes a critical issue in developing legal rules for electronic commerce. This paper takes a position not inconsistent with this DoD draft position. In further support, consider the technical characteristics of *datagrams* -- self-contained packets that do not require acknowledgments. See WILLIAM STALLINGS, DATA AND COMPUTER COMMUNICATIONS 564 (McMillan 1985). "In the datagram model, the network layer simply accepts messages from the transport layer and attempts to deliver each one as an isolated unit. Messages may arrive out of order, or not at all." ANDREW A. TANNENBAUM, COMPUTER NETWORKS 188 (Prentice Hall 1981).

³⁸ E.C. *supra* note 6 at Annex, Action Line 3.1. "Any Electronic Signature capability should ideally be able to serve several distinct needs at the same time related to different and independent applications or service providers. It should ideally provide the capability of being a universal information and communication carrier, allowing *mobile interworking using an open systems approach*." DG XIII, COMMISSION OF THE EUROPEAN COMMUNITIES, REFLECTION NOTE ON POSSIBLE COLLABORATION IN THE FIELD OF ELECTRONIC SIGNATURE THE KEY TO MOBILITY, RA920007 (May 27, 1992) at 2 (emphasis added).

Increasingly in response to the vagaries of open systems, trading partners have sought to contract with their respective third party service providers to obtain periodically provider's independent audit reports. One purpose of this private contracting is to substitute such reports for the trading partner's audit of the external "open" environment. However, a recent decision may diminish the utility or advisability of this practice. See *Bily v. Arthur Young & Co.*, 11 Cal.Rptr.2d 51 (Sup. Ct. 1992) (holding that an auditor owes no general duty of care regarding the conduct of an audit to persons other than the client except where the audit was intended to benefit a third party [a trading partner] and where negligent misrepresentation was based on actual and justifiable reliance).

³⁹ E.C., *supra* note 6, Action Line 4.1. ("In the security of information systems there is inherently a very close relationship between regulatory, operational, administrative and technical aspects.") The adoption and use of security procedures are also pivotal for determining risk shifting for unauthorized payment orders under U.C.C. Art. 4A which deals with funds transfers. Note the scheme of presumptions in U.C.C. Art. 4A reprinted in note 45, *infra*. See *infra* Section IV. BURDEN OF PROOF AND PRESUMPTIONS. "An all-electronic ACH Network would result in a higher level of security for all ACH payments . . . The reserve banks currently offer data encryption. . ." Federal Reserve Bank Services, 55 FED. REG. 53,051-01 (Dec. 26, 1990).

studies and opinions of public and private entities. For example, the United Nations Commission on International Trade Law (UNCITRAL) stated that "it is clear that the legal reliability of EDI techniques requires that high standards be used to determine legal certainty as to the identity of the sender, its level of authorization and the integrity of the message."⁴⁰ The Comptroller General of the United States has remarked that "[a]gencies can create valid obligations using *properly secured* EDI systems."⁴¹

Other supporting opinions can be seen in model trade agreements and the developing literature. A model EDI agreement states that "[a]dequate security procedures are recognized. . . as critical to the efficacy of electronic communication. . . . The use of adequate security enhances the reliability of those records and enhances the ability to prove the substantive terms of any underlying commercial transaction."⁴² A further supporting view notes that "[l]egal reliability actually implies 'demonstrably and unarguably high standards of authorization, [sic] operational and access control and management' use of IACT [information and communication technology] systems. 'Authorisation,' further, implies 'accurate, precise and dependable identification, verification and authentication technologies and techniques which are, or may become, as legally acceptable as the conventional trust and comfort of a manual signature written in ink on paper.'"⁴³

⁴⁰ *Electronic Data Interchange*, Rep. of the Sec. Gen., UNCITRAL, 246th Session, Vienna, 10-28 June, 1991, U.N. Doc. A/CN.9/350 (15 May 1991) at 23. Also, a recommendation by UNCITRAL that was endorsed by the UN's Gen. Assembly called ". . . upon Governments and international organizations to take action, where appropriate, in conformity with the Commission's recommendations so as to ensure *legal security* in the context of the widest possible use of automated data processing in international trade." Resolution 40/71, ¶ 5(b) U.N. Doc. A/40/17 (11 Dec. 1985). (emphasis added).

⁴¹ Dec. of the Comp. Gen., *supra* note 27 (emphasis added).

⁴² A MODEL EDI TRADING PARTNER AGREEMENT § 1.4 Comment 1, *supra* note 14. The implementation of security is more than just an exercise of wisdom by an entity adopting such procedures or policies, but may, as discussed in this paper, effect the legal efficacy of the electronic transactions and records.

⁴³ Stephen Castell, "The Legal Admissibility of Computer Generated Evidence Towards 'Legally Reliable' Information and Communications Technology (IACT)," COMP. LAW AND SEC. REP. (Jul.-Aug. 1989) at 7-8. (discussing the Appeal Study *Appendix on Evidence Admissible in Law* by S. Castell and the Central Computer and Telecommunication Agency, British Treasury, 1988; subsequently published as The Appeal Report, May, 1990).

b. Reasonable Security Procedures

Unlike conventional paper-based transactions and records, there is little jurisprudential guidance as to whether (and, if so, under what circumstances) a particular security technique, procedure or practice will provide the requisite assurance of reliability in electronic form. This lack of guidance concerning security is reflected in the multiplicity of current security and authentication practices within the EDI community. These practices, in many instances, appear to have been implemented in an *ad hoc* manner, with neither a clear understanding of the present state of law, nor the technical proof assurances of other chosen practices.⁴⁴ Where the law has responded, it has been arguably too vague -- such as a requirement to implement *reasonable security procedures*.⁴⁵

While security procedures should certainly be reasonable, in certain situations a lack of specificity in defining "reasonable" security procedures may provide inadequate guidance causing such security

⁴⁴ In a survey of EDI users, the mechanisms or procedures employed as legal signatures included the following: a "buyer code," a DUNS number and suffix, a password, a message authentication code, an account number, an ID/password combination, an "electronic verification of symbol and codes," and functional acknowledgments. LEGAL AND BUSINESS CONTROLS TASK GROUP, ACCREDITED STANDARDS COMMITTEE X12, 1990 SURVEY (1990). The law should be flexible in permitting a variety of signatures in electronic form. However, this survey reflects a lack of purposeful, consistent and knowledgeable choices by the user community, as well as the law's lack of clarity.

⁴⁵ For example, in banking, a *security procedure* has been defined as: "a procedure established by agreement of a customer and a receiving bank for the purpose of (i) verifying that a payment order or communication amending or canceling a payment order is that of the customer, or (ii) detecting error in the transmission or the content of the payment order or communication." U.C.C. § 4A-201 "Security Procedure."

"Commercial reasonableness of a security procedure is a question of law to be determined by considering the wishes of the customer expressed to the bank, the circumstances of the customer known to the bank, including the size, type, and frequency of payment orders normally issued by the customer to the bank, alternative security procedures offered to the customer, and security procedures in general use by customers and receiving banks similarly situated. A security procedure is deemed to be commercially reasonable if (i) the security procedure was chosen by the customer after the bank offered, and the customer refused, a security procedure that was commercially reasonable for that customer, and (ii) the customer expressly agreed in writing to be bound by any payment order, whether or not authorized, issued in its name and accepted by the bank in compliance with the security procedure chosen by the customer." U.C.C. § 4A-202(c) (Authorized and Verified Payment Orders).

procedures to fail in their intended purpose. . . . Specificity may help the parties implement and comply decisively and unambiguously with security procedures, reduce confusion and offer better expectations of reliability and certainty. Security procedures should be sufficiently precise so that they are not subject to discretionary, self-serving interpretation, in part, because: (i) few standard security procedures exist in the law. . . . (ii) security technology is changing rapidly, and (iii) parties often hold particularly diverse opinions on appropriate solutions to security threats.⁴⁶

One difficulty in developing responsive laws involves deciding the extent to which law should detail and endorse particular security techniques, procedures or practices.⁴⁷ Proponents of specificity argue that the electronic commerce community needs greater guidance⁴⁸ and that private agreements and legislation requiring only *reasonable security procedures* are vague and unworkable. Proponents of generality, on the other hand, argue that the endorsement of specific security procedures, practices or techniques leads to inflexibility and creates a presumption that the failure to implement such techniques, procedures and practices constitutes failure to exercise ordinary care. While recognizing

⁴⁶ MODEL ELECTRONIC PAYMENTS AGREEMENT AND COMMENTARY, § 7 Comment 5, (June, 1992), prepared by the EDI and Information Technology Division, Section of Science and Technology, American Bar Association, (hereinafter "MODEL AGREEMENT") 32 JURIMETRICS J. No. 4 at 601 *et seq.* (1992)) (the Model Agreement is available from the ABA's Order Fulfillment Department, Chicago, IL -- Product Code 545-0009; *see dicta* in *Banque Worms v. Bank America*, 726 F.Supp. 940 (S.D.N.Y. 1991) (querying whether the courts will be able to determine commercial reasonableness with their present tool set). *See generally*, Michael S. Baum, *Commercially Reasonable Security: A Key to EDI Enforceability*, ACTIONLINE, (AIAG, Nov. 1989), and *Computer Law & Practice* (Vol. 6, No. 2, 1989) at 52-54.

⁴⁷ Various legislation and guidelines mentions, or recognizes specific security technologies, including, *e.g.*, *encryption* in U.C.C. § 4A-201, and UNCID Art. 9(a). Where technologies are specified for descriptive purposes or by attribute and they will not cause legislation to fail in its intended purpose.

⁴⁸ "Buyers of cryptography cannot independently evaluate a seller's claims of product security." Sandy Epstein, "Striking a Balance: View on a National Cryptographic Policy," testimony before the National Computer System Security and Privacy Advisory Board, NIST (Gaithersburg, Sept. 1992). Also, the concerns and requirements of security users tend to demonstrate their preference toward specificity. One recognized security professional said, "[i]f, by chance, we ended up in a litigation situation, I want my case to be backed by the argument that I'm using the best system and one that's sanctioned by the government." Sandra Lambert, VP Information Security, Citibank, N.A., as quoted in *Network World* (Sept. 28, 1992) at 28.

these competing interests, a stronger viewpoint supports a measured movement toward greater specificity.

The electronic commerce community is asking lawyers to consider and to provide advice concerning signatures, security procedures and other related issues, but as yet, the legal community's experience with these issues is limited. Attorneys often defer to security professionals, who in turn seek the guidance of auditors, who then defer to attorneys. This *circle of deference* suggests that sufficiently concise answers to, responsibility for, and the resolution of, these issues are not quickly forthcoming. Moreover, it suggests that there is need for professional education in the system.⁴⁹ Further study is warranted in this area. Lawyers, security professionals and auditors should strive to provide education as a means to develop ideas on what attributes reasonable security would possess, as well as to identify responsive security services, their associated strengths, and when they can and should be implemented.

Consistent with this approach, the House of Delegates of the American Bar Association (ABA) has approved the first ABA Resolution that directly responds to critical legal-security issues affecting electronic data interchange and electronic commerce. The resolution requires the ABA to do the following:

[s]upport action by federal and state governments, international organizations, and private entities to:

- a) facilitate and promote the orderly development of legal standards to encourage use of information in electronic form, including appropriate legal and professional education;
- b) encourage the use of appropriate and properly implemented security techniques, procedures and practices to assure the authenticity and integrity of information in electronic form; and
- c) recognize that information in electronic form, where appropriate, may be considered to satisfy legal requirements regarding a writing

⁴⁹ There are only a few formal law school course offerings applicable to computers and EDI legal issues and course offerings on information security legal issues are probably nonexistent. "A lack of EDI education is perhaps today's greatest hindrance to productive EDI usage and such implementation." Sokol, *EDI Education Pays Dividends*, Data Interchange (Dec. 1991) at 16. "One simple but effective response is education. . . many security dilemmas can be redressed through proper training and administration." *The Bigger the Network, the Scarier*, INFORMATIONWEEK (Sept. 7, 1992) at 44.

or signature to the same extent as information on paper or in other conventional forms *when appropriate security techniques, practices, and procedures have been adopted*.⁵⁰

Consistent with the ABA approach, the United Nations Commission on International Trade Law ("UNCITRAL"), as early as 1985, recommended that governments "review legal requirements of a handwritten signature or other paper-based method of authentication on trade related documents with a view to permitting, where appropriate, the use of electronic means of authentication."⁵¹

c. Mapping Security Attributes to Legal Standards

There are various techniques available, with specified assurances to authenticate the source of, verify the content of, and control access to, data in electronic form. Many more of these techniques will develop as both the technology and the law evolve. History has demonstrated repeatedly that legal rules prescribing technology for authentication and related purposes have been a function of the available technology, historical accident or anomaly, and the technology's forensic⁵² characteristics. It has also been transitory.⁵³

The following table (TABLE 1) presents some of the attributes of conventional writing and signings as compared to their *approximate* electronic security analogs. The strength (and the propriety of the suggested analog) of any such security mechanism depends considerably on its implementation and the associated system controls. For example, in the case of a "signature" requirement, any appropriate security technique that provides comparable or superior attributes to those produced by the conventional use of a written signature

⁵⁰ Developed and submitted by the Section of Science and Technology to the House of Delegates of the ABA, the Resolution (no. 115) was approved on Aug. 19, 1992 (emphasis added).

⁵¹ OFFICIAL RECORDS OF THE GENERAL ASSEMBLY, FORTIETH SESSION, SUPPLEMENT NO. 17 (A/40/17), ¶ 360.

⁵² See generally, BAUM, EDI AND THE LAW, *supra* note 11 § 9.4 "The Signing Requirement" at 123-125 (asserting that signatures and their electronic analogs should carry "forensic characteristics providing probative evidence of identity").

⁵³ See Preface, *supra* (providing quotes that give insight into the forensic and transitory nature of technology-related rules).

should be satisfactory.⁵⁴ However, the various security attributes in TABLE 1 demonstrate that the handwritten signature does not have an unequivocal electronic analog.⁵⁵

⁵⁴ Conventional paper-based handwritten signatures inherently have security attributes to the extent that, *e.g.*, ink cannot easily be erased without detection, paper is non-transient, and a signature is biometrically unique. Aside from these attributes, "[t]he qualities of the *ink* or *paper* or *type* of a document are proper indicia to consider in investigating the genuineness or the age of a document, and expert testimony may be employed to aid in this." 7 J. WIGMORE, EVIDENCE § 2024 (Chadbourn rev. 1981) (hereinafter "WIGMORE"). Notwithstanding, it has been recognized that conventional signatures are "far from the most efficient or the most secure method of authentication." UNCITRAL at ¶ 64. Note, *Digital signatures . . . could fulfill the essential functions of the orthographic signature*. COMMISSION OF THE EUROPEAN COMMUNITIES, TEDIS, THE LEGAL POSITION OF THE MEMBER STATES WITH RESPECT TO ELECTRONIC DATA INTERCHANGE, (Brussels, Sept. 1989) at 305.

⁵⁵ These three examples of information in electronic form (categories "B," "C" and "D" in TABLE 1) are also used to support the security services provided in the Model Security Baseline in Section III.c., *infra*.

	A	B	C	D
ATTRIBUTE	CONVENTIONAL SIGNED WRITING COMMUNICATED VIA UNITED STATES POSTAL SERVICE	UNENCRYPTED INFORMATION WITH SYMBOL IN ELECTRONIC FORM COMMUNICATED VIA THIRD PARTY SERVICE PROVIDER	DIGITALLY SIGNED OR COSIGNED INFORMATION IN ELECTRONIC FORM ⁵⁶ COMMUNICATED VIA THIRD PARTY SERVICE PROVIDER	DIGITALLY SIGNED & NOTARIZED INFORMATION IN ELECTRONIC FORM COMMUNICATED VIA THIRD PARTY SERVICE PROVIDER
Origin Authen.	Medium-Strong	Weak	Strong	Strong
Proof of Receipt	Return Receipt	Weak	Strong	Strong
Content Integrity	Partial	Weak	Strong	Strong
Time of Creation	Weak	Weak	Weak	Strong
Time of Dispatch	Postmark	Weak	Weak	Strong
Time of Receipt	Return Receipt	Weak	Weak	Strong
Time of Acknow.	Return Receipt	Weak	Weak	Strong
Singularity	Yes	No	No	Can be offered as a "registry" service
Biometric	Yes, signature	No, but available for resource access control	No, but available for resource access control and for cryptoignition ⁵⁷	No, but available for resource access control and for cryptoignition
Expression of Intent ⁵⁸	Indicia	Indicia	Indicia	Indicia
Non-repudiation	Partial	Weak	Strong, except time	Strong
Privacy	If enveloped ⁵⁹	Weak	Weak	Weak

TABLE 1 - COMPARISON OF SIGNED WRITINGS AND ELECTRONIC INFORMATION*

⁵⁶ While many security services are best implemented using digital signatures or comparable cryptographic methods, many can be implemented non-cryptographically, although not necessarily with comparable economy, strength, functionality or elegance.

⁵⁷ A quantity which enables a cryptographic algorithm(s) or device embodying a cryptographic algorithm(s) to operate which is generally implemented as a component of a secret quantity used to convert other quantities necessary for operation.

⁵⁸ This may vary among criminal and civil proceedings.

⁵⁹ "The Postal Service must preserve and protect the security of all mail in its custody from unauthorized opening, inspection, or reading of contents or covers, tampering, delay or other unauthorized acts." DOMESTIC MAIL MANUAL (DMM) § 115.1 "Importance of Mail Security;" "In general, no person may open, read, search, or divulge the contents of mail sealed against inspection . . ." DMM § 155.21 "Opening, Reading, and Searching Sealed Mail Generally Prohibited."

Key to TABLE 1

* General Comment: Attributes exhibiting a propensity for forgery are listed as "Weak."
 TABLE 1 includes subjective positions and is intended exclusively for pedagogical purposes.
 A: A signed paper document sent by postal service.
 B: Unencrypted (clear text) communicated via third party service provider (TPSP).
 Satisfaction of many listed attributes depends largely on controls, including TPSP controls.
 C: Digitally signed electronic document.
 D: Digitally signed electronic document which is "notarized" (time stamped and digitally signed) by a trusted third party. In this Table, notarization is available (via *trusted box*) at the site of origin, at the respective TPSPs and at the site of receipt.

One additional comparison is instructive. A decision of the Comptroller General proffered three signature attributes as being necessary to create obligations which can be recorded against the government.⁶⁰ TABLE 2 considers these attributes within the context of fallibilities of paper-based media.⁶¹

PROPOSED SIGNATURE ATTRIBUTES ⁶²	FALLIBILITIES
Unique to the Certifying Officer	Forgery. Where stamps and other mechanisms are used, the signature is not unique to the certifying officer.
Capable of Verification	Error prone. Signature comparison is an art as well as a science; verification often disregarded due to cost, ineffectiveness or unavailability.
Under Officer's Sole Control	Law permits other mechanisms which may not, without knowledge of custom and practice, provide assurances of sole control.
<i>Proposed effect:</i>	
Demonstration of Intent to be Bound ⁶³	Depends on the circumstances of its use. Not an inherent attribute.

⁶⁰ See *supra* note 27, (citing and describing the relevant Decision).

⁶¹ Cf., the quotes in the Preface to this paper concerning fallibilities of conventional media.

⁶² Proposed by the Comptroller General of the United States.

Other signature attributes which have been proposed within the private and commercial sectors include attributes that: *identify* the signatory to the transaction; *demonstrate* that the signatory had the intent to formalize the information due to its importance; *create* a record acceptable to the dispute resolution mechanism; *evidence* the existence of a contract; and, *prevent* repudiation.

TABLE 2 - FALLIBILITIES OF PAPER-BASED SIGNATURES

To the extent, *arguendo*, that the Comptroller General's decision is interpreted to substantially require the use of cryptographic methods⁶⁴, three observations deserve consideration. First, despite an inference that paper-based signatures provide a good benchmark for authentication and provability, Table 2's proffered signature fallibilities effectively present a compelling case that supports the permissibility of non-cryptographically enhanced transactions where appropriate.⁶⁵ Second, the noted weaknesses of conventional signatures relative to digital signatures (*see* TABLE 1) support the legal efficacy of digital signatures in substitution for the latter. Third, although the decision does not expressly reference *non-repudiation*, it effectively focuses on the attributes of non-repudiation, thereby bolstering the utility of this comparatively unfamiliar service.

⁶³ This is not a formal attribute but instead a conclusion. Note also that some government representatives advocate that having established a signature, it is also necessary to demonstrate that the signature is *linked to the data*.

⁶⁴ Cryptography "embodies principles, means and methods for the transformation of data in order to hide its information content, prevent its undetected modification and/or prevent its unauthorized use." ISO 7498-2-1988(E) § 3.3.20. Security standards that implement cryptographic methods are available for various applications including EDI (ANSI X12.58 "Security Structures"), banking (ANSI X9.17 "Financial Institution Message Authentication (Wholesale)") and government (FIPS-PUB 113 "Computer Data Authentication"). Cryptographic standards are either available or in development that utilize more recently developed security technologies, such as *public key* cryptography that uses *digital signatures*. *See* NIST, A PROPOSED FEDERAL INFORMATION PROCESSING STANDARD FOR DIGITAL SIGNATURE STANDARD (DSS), 56 Fed. Reg. 42,980 (Aug. 30, 1991); and NRC, *supra* note 32 at 252-261 (distinguishing private and public cryptosystems as well as a recognized DSS alternative -- RSA). *See* Michael S. Baum, THE PROPOSED DIGITAL SIGNATURE STANDARD: IMPLICATIONS FOR ELECTRONIC COMMERCE, COMP. L. & SEC. REP. Vol. 8, Issue 3, (Elsevier, UK, Sept.-Oct. 1992) at 217-225.

In further support of the appropriate use of technology-based solutions, *see* FINANCIAL MANAGEMENT SYSTEMS, OMB Circular No. A-127 (obliging government agencies to *use the most contemporary technology*); and T. J. Hooper, 60 F.2d 737 (1932) ("[a] whole calling may have unduly lagged in the adoption of new and available devices").

⁶⁵ *See infra* Section III.c. "A Model Security Baseline."

d. **Non-Repudiation**

Some security services can provide diverse capabilities that are not necessarily provided by conventional paper-based techniques. One such security service is known as a *non-repudiation service*. Generally, non-repudiation services prevent a document's originator from denying the document's origin and provide *irrevocable proof of authenticity*.⁶⁶

The Non-repudiation Service may be provided through the use of mechanisms such as digital signatures, encipherment, data integrity and notarization, with support from other system services such as Time Stamping and Security Services. The Non-repudiation Service can use a combination of these mechanisms and services as appropriate to satisfy the security requirements of the application in question. The goal of the service is to collect, maintain, make available and validate non-deniable proofs regarding data transfers between the originator and recipient.⁶⁷

A non-repudiation service is presented as *one* example of a security service, which, whether or not cryptographically based, may satisfy requirements that are linked to conventional writings and signings, such as contributing to evidence of a party's intent to contract or to be bound. Although many existing legal requirements do not require absolute or non-repudiable proof, these security services offer the legal and control communities important tools and possibilities with which to fashion legal obligations to accommodate electronic practices (particularly the more important or risky obligations).

The time of the creation of a transaction or the submission of a transaction to an electronic messaging system, or the time when received or retransmitted by a third party service provider (TPSP), available to, received by, or acted upon by the intended recipient is critical in various applications. For example, where parties must file information electronically⁶⁸ (e.g., tax returns), or where an

⁶⁶ MESSAGE HANDLING: EDI MESSAGING SERVICE, CCITT Draft Rec. F.435 (Version 5.0, June 15, 1990).

⁶⁷ ISO/IEC JTC1/SC21, Intro., WORKING DRAFT NON-REPUDIATION FRAMEWORK, N7082, Project 97.21.49.6 Q53 (July 1992).

⁶⁸ The definition of *filing* has come under review. [insert references and relation to receipt and model agreements.]. "The word *file* is derived from the Latin work 'filum,' and relates to an ancient practice of placing papers on a thread or wire for safe-keeping and ready reference. Filing, it must be observed, is not complete until the document is delivered and received. "

electronic bidding process closes at a time certain, or where the first to file a response wins⁶⁹; trusted time stamping is recognized as a prerequisite to the proof of the completion of obligations of one party, and the transfer of obligations to another.

Despite the great benefits enuring from the use of digital signatures, they have some inherent limitations (as is true with any security mechanism) including an innate inability to provide "time-related" non-repudiation. Digital signatures and other cryptographic methods cannot, in the absence of a trusted entity, provide an unforgeable trusted time stamp. Therefore, to achieve *full* non-repudiation, time stamping must be undertaken by a disinterested party beyond the control of the parties to a transaction or record. Such a third party is a trusted entity.

e. Trusted Entities and Time Stamping

A trusted entity is an independent, unbiased entity capable of providing important security assurances that enhance the enforceability and reliability of electronic records. The key attributes of a trusted entity are that it is a *disinterested, unbiased, third party* trusted by the parties to the transaction and by the dispute resolution mechanism(s) relevant to a transaction or record. Simply stated, a trusted entity's administrative, legal, operational and technical infrastructure must be beyond reproach.⁷⁰

U.S. v. Lombardo, 36 U.S. 508, 509 (1916) (violation of statute making it a crime for the harbinger of an alien woman for purposes of prostitution to fail to file with Immigration). See MICHAEL S. BAUM AND HENRY H. PERRITT, JR., ELECTRONIC CONTRACTING, PUBLISHING AND EDI LAW (Wiley, 1991) [hereinafter "Baum and Perritt"] at § 5.16 "UCC Security Interest Filings" (considering many electronic filing issues).

⁶⁹ See *Abourezk v. Federal Power Commission*, 513 F.2d 504, 505 (D.C. Cir. 1975) (where Judge Bazelon noted that "[d]ue to lack of synchronization between the clocks in the clerks' offices and those in the offices of the various federal agencies, it is often not possible to be certain which petition was the first to be filed after the agency entered its order.")

⁷⁰ Third Party Service Providers or value added networks, such as ATT or MCI (collectively "VANs") have arguably been inaccurately identified as trusted entities. VANs are not necessarily disinterested because they may compete with each other, participate in the transfer or processing of information (and therefore have exposure), and may introduce error, delay, unavailability or misdelivery. Query whether VANs should inherently be trusted.

A trusted entity can time and date stamp,⁷¹ store (or forward) a "record copy" or hash of a transaction, keep an audited data log, or serve as an intermediary for other trust-based services between trading partners.⁷² The trusted entity's record copy of an electronic transaction would control in the event of a dispute regarding a document's authenticity or timeliness.

The electronic notary⁷³ offers unique solutions to one of the critical "missing links" of electronic transactions and records assurances: unforgeable trusted time stamping. The electronic notary also may facilitate future TPSP and

⁷¹ The author offers a French term, which more concisely describes the intended time stamp functionality: *horodatage* (horo=hour, and datage=date). The use and significance of time stamping has both a rich historical as well as contemporary value. See *Hill v. Bache Halsey Stuart Shields Inc.*, 790 F.2d 817 (10th Cir. 1986) (failing to time stamp order tickets during or soon after trader's conversation with his client was violation of Commodity Futures Trading Commission Rule). "(i) Each Futures commission merchant . . . receiving a customer's . . . order shall immediately upon receipt thereof prepare a written record of such order, including the account identification and order number, and shall record thereon by time-stamp or other timing device, the date and time, to the nearest minute, the order is received. . . ." 17 C.F.R. § 1.35(a)(a-1); *Toppo et al.*, 474 F.Supp. 48 (Bankr. D.PA 1979), "Absent contrary evidence, Pennsylvania Department of State Time Stamp on financing statements controlled the order of filing, notwithstanding the fact that the later filed statement was given number earlier than that given to previously filed statement." 12A P.S. § 9-302(1); *Carlos v. N.Y. State Dept. of Taxation*, 531 F.Supp. 359, 269-270 (D.N.Y. 1981) (time stamp of county clerk is time of filing); *Old Colony Donuts v. American Broadcasting Companies, Inc.*, 368 F.Supp. 785 (D.MA 1974) (court's time stamp on complaint barred action due to tolling of statute of limitations); *Interstate Commerce Commission v. Travelers Motor Freight, Inc.*, 195 F.Supp. 267 (D.VA 1961) (tightened procedures (for compliance with ICC regulations for a certificate by improving register-log of drivers) by requiring a time stamp to be affixed to the register and the initials of an employee of the Service Station, and "since these more strict requirements had been made effective, no violations of the gateway had occurred."); 48 C.F.R. § 513, 57 Fed. Reg. 26,608 (June 15, 1992) (time-stamping of invoices to indicate receipt date as precondition to payment); see also FED. R. CIV. P. 6 "Time" (providing a detailed scheme for computation of time periods under the rules); and U.C.C. § 1-204; U.C.C. § 4A-210 "Rejection of Payment Order", Official Comment 2). Consider whether the electronic notary could provide useful assurances within the context of the EXPEDITED FUNDS AVAILABILITY ACT, 12 U.S.C. § 4001, *et seq.*, REG. CC, and 12 C.F.R. § 229.10(b).

⁷² See BAUM AND PERRITT, *supra* note 68 at Ch. 5 (providing an extensive survey of possible trusted entity - clearinghouse services).

⁷³ The terms "notary" or "notarization" in the context of electronic transactions do not have recognized legal standing equivalent to that of the conventional notary public, and consequently, such terminology used in this setting is inaccurate or potentially confusing. See BAUM AND PERRITT, *supra* note 68 §§ 4.33-4.36 (presenting a survey of issues pertinent to the automation of the notary public).

value added network service requirements by providing them with trusted-entity services.⁷⁴ The electronic notary can provide irrefutable proof of the time of the origination of the document.⁷⁵ Notarizing data intended for record retention and archiving provides an unforgeable seal which may contain a time stamp and digital signature, together with additional audit, legal and security information intended to enhance its legal efficacy.⁷⁶

III. RISK ANALYSIS AND RISK-BASED APPROACHES

a. Risk Analysis

To the extent that various methods to assure that reasonable security procedures have been considered and implemented in both the private and public sectors, results have been inconsistent -- just as attempts to satisfy amorphous requirements for *commercially reasonable security* have produced varying results.⁷⁷ Such inconsistent results are explained, in part, by the insufficient and varying analytical tools used to evaluate security requirements (and their legal efficacy), such as *risk analysis*.

'Risk analysis' is a procedure used to estimate potential losses that may result from system vulnerabilities and the damage from the occurrence of certain threats. Risk analysis identifies not only critical assets [and processes⁷⁸] that must be protected but considers the environment in

⁷⁴ Because the electronic notary is not controlled by TPSPs or VANs, reliance by users need not be placed exclusively on the internal controls of the TPSPs and VANs, except for availability.

⁷⁵ Cf., the proofs available from an electronic notary to those available from the U.S.P.S.. For example, consider that "[m]ail deposited in a collection box or post office may, with proper identification, be recalled by the sender." DMM *supra* note 59 at § 152.71 "Who May Recall Mail;" and "[p]ost offices must honor requests for "handback" cancellation service where a customer personally presents an addressed or unaddressed envelope. . . to a postal clerk for cancellation with the current day's postmark and immediate return or handback to the customer." DMM § 164.23(1) "Handback Service."

⁷⁶ See *supra* note 67 (WORKING DRAFT NON-REPUDIATION FRAMEWORK).

⁷⁷ See *supra* Section II.b., Reasonable Security Procedures.

⁷⁸ See Thomas A. Stewart, "The Search for the Organization of Tomorrow," *Fortune*, (May 18, 1992) at 94-94 (includes a proposal for viewing the organization horizontally by core

which these assets are stored and processed. The ultimate purpose of risk analysis is to help in the selection of cost-effective safeguards that will reduce risks to an acceptable level.⁷⁹

The National Institute of Standards and Technology ("NIST") noted the need for EDI risk analysis in March 1991 when it required agencies to *employ risk management techniques*. Yet, NIST did not provide specific guidance on EDI risk analysis.⁸⁰ The creation and enforcement of legal commitments undertaken electronically may require new criteria (such as EDI-relevant legal criteria) and approaches to risk analysis that have either not been developed or widely adopted.⁸¹ For example, EDI may involve variables and *higher order effects* that are difficult to quantify and that effectively require consideration of the legal interrelationship between a series of related EDI transactions and records without direct conventional analogs.⁸² "EDI/EFT is too young for its full risk implications

processes -- each core process is a set of functions necessary to meet a major external objective such as inventory turnover or on-time delivery. Three examples of core processes which hold incrementally increasing risks are presented: first, generation and fulfillment of ordinary business transactions; second, integrated logistics (arguably sophisticated electronic commerce); and third, future market share.

⁷⁹ IRENE GILBERT, GUIDE FOR SELECTING AUTOMATED RISK ANALYSIS TOOLS, NIST Special Pub. 500-174 (1989) at 3. THE COMPUTER SECURITY ACT OF 1987, 40 U.S.C. § 759 note, P.L. 100-235 (1987), requires applicable federal agencies to develop a computer security and privacy plan "that is commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information contained in" each Federal computer system. The Act's focus on risk, rather than on formalism, presents important considerations for future viable legislative and regulatory approaches to important issues raised in this paper.

⁸⁰ NIST, ELECTRONIC DATA INTERCHANGE (EDI), FIPS-PUB 161, 56 Fed. Reg. 13,123 (Mar. 29, 1991). *Cf.*, NIST COMPUTER SYSTEMS LABORATORY (CSL) BULLETIN, SECURITY ISSUES IN THE USE OF EDI (June, 1991).

⁸¹ Existing risk analysis tools focus neither on legal requirements nor on the particular needs of EDI. *See* NIST, GUIDELINE FOR AUTOMATED DATA PROCESSING RISK ANALYSIS, FIPS PUB 65 (Aug. 1979). *Cf.*, Birch and McEvoy, "A Structured Approach to Information Security Risk," COMP. LAW & SEC. REP., Vol. 8 Issue 4 (Jul.-Aug. 1992) at 177.

⁸² *E.g.*, EDI Functional Acknowledgment and Application Advice transaction sets do not exist in conventional paper-based practices. The loss or garbling of such transaction sets present challenges to conventional risk analysis. *See* BAUM AND PERRITT, *supra* note 68 at 180-181. Also, consider the difficulty of assessing lost profits caused by intermittent system interruption or performance degradation.

to become apparent."⁸³ There should be a move toward the development of authoritative risk analysis for electronic commerce in both the private and public sectors.

b. Security Baseline Issues

In considering various approaches to linking technical security measures and the law, it is important to recognize that the strength and reasonableness of security procedures for particular applications are risk driven. These procedures, therefore, must undergo further scrutiny. A *security baseline*⁸⁴ ("baseline") is a tool that may help define and rationalize security requirements for diverse electronic transactions and records. A baseline serves as a foundation to develop a clear expression of security requirements, facilitate open trading environments, ensure that transaction costs are commensurate with the risks, and provide greater legal certainty.⁸⁵

A baseline can encompass generally accepted security methods and procedures (to the extent available to attain reasonable security at the operating system, data communication, and application (including EDI) levels).⁸⁶ Compliance with such requirements would establish a presumption of the

⁸³ David Davies, "EDI Insurance - The 'Red Herring' Theory Examined," CLSR, Vol. 8, Issue 5 (Sept.-Oct. 1992) at 226-229 (noting "the relatively unproven or un-demonstrated nature of the risks;" and that "very little reliance should be placed upon the ability of existing insurances to encompass the new risks of EDI").

⁸⁴ See Baum, Actionline, *supra* note 46 at 35 (advocating a security baseline).

⁸⁵ The approach to the development of a baseline should be examined cautiously, considering that "[t]he law embodies the story of a nation's development through many centuries, and it cannot be dealt with as if it contained only the axioms and corollaries of a book of mathematics." OLIVER WENDELL HOLMES, THE COMMON LAW *supra* note 1; and also taking into consideration that we should not take too *formulaic* an approach. However, in balance, a baseline responds to a clear need, and no better tool has yet been identified. Note, concerning FIPS-PUB 140-1, "[f]ew know what level of information or risk of loss should be equated to each of the levels of the protection described in the standards." Sandy Epstein, *supra* note 48.

⁸⁶ See NRC, *Recommendation 1 Promulgate Comprehensive Generally Accepted Security System Principles (GSSP)* *supra* note 32 at 27-32. The following is a list of examples: quality control, access control code, user identification and authentication, protection of executable code, security logging, security administrator, data encryption, operational support tools, independent audit and hazard analysis. *id.* at 28-29.

security procedure's sufficiency or legal efficacy.⁸⁷ A Baseline can take various forms, including legislation, private agreement and guidelines.⁸⁸

The purpose of a baseline is to serve as a bridge between high-level policy and philosophical positions on one end of the spectrum, and, at the other extreme, detailed application-specific rules. As such, a baseline is positioned at an intermediate level of abstraction which both seeks to enforce high-level policy and provides a mechanism for the development of workable rules. TABLE 3 provides one perspective on how a baseline can be used and where it fits into the legal-standards environment.

ABSTRACTNESS	TYPE	COMMENTS
High	"Reasonable Security Procedures"	Too uncertain for rules; Preferably a policy objective
Medium	Baseline (single or multilevel)	A tool to help enforce policy objectives
Low	Application-specific rules and guidelines	Compliant with Baseline

TABLE 3 - RELATIVE LEVELS OF ABSTRACTION

Baseline security requirements should vary depending on risks and on other factors.⁸⁹ For low risk transactions -- *such as* those with a low probability of large losses, the benefits of strong security are likely outweighed by the costs of such measures.⁹⁰ Higher risk transactions may require more stringent controls, including cryptographic methods or trusted entity services.

⁸⁷ See *infra* Section IV. BURDEN OF PROOF AND PRESUMPTIONS (presenting an alternative to the legal effect of the Model Baseline in TABLE 6).

⁸⁸ See BAUM AND PERRITT, *supra* note 68 at 80-81 (discussing various forms of implementation guidelines).

⁸⁹ See the various factors described later in this section.

⁹⁰ For most electronically communicated commercial non-financial transactions, the security regime is typically little more than that provided by simple password/ID-based access or authentication controls. Such weak security probably results from established customs and practices, simplicity, lack of security sophistication, financial constraints, and the belief that password/ID-based access controls are the lowest common denominator (and, in this respect, are most pragmatic) for ubiquitous computer-based communications.

A baseline should be sufficiently concise without regard to risk.⁹¹ The more specific the baseline, the greater will be the transactional certainty, user confidence, and ultimate success. Without specificity, security requirements may provide inadequate guidance and may fail in their intended purpose.⁹² Specificity helps users to implement decisively and to comply unambiguously with baseline requirements. Consequently, until the parameters of *reasonable security* practices in electronic commerce become more clearly defined (as a function of improved experience and practice coupled with the use of better risk analysis tools), greater specificity is advocated. A baseline arguably fills this gap. Thereafter, generalized or abstract standards of "reasonable security" may become legally sufficient -- in an environment benefiting from legal precedent, and widely recognized specific procedures and practices.⁹³

In order to understand this idea, the following issues should be considered in developing a baseline (but not necessarily be limited to):

1. Attribute-based Security Requirements - The security of particular transaction types, and of a particular transaction, will depend upon the needed security services and will vary as a function of risk and legal needs. Security services include authentication, integrity, non-repudiation, confidentiality, and availability.⁹⁴ TABLE 1, *supra*, presents security attributes within the context of a comparison to paper-based mechanisms.
2. Value Requirements - Developing consensus on a definition of value⁹⁵ is becoming a focal point in the development of electronic commerce rules⁹⁶ in

⁹¹ See *supra* note 48, (concerning needed specificity in security procedures).

⁹² See Michael S. Baum, *Commercially Reasonable Security: A Key to EDI Enforceability*, Actionline, *supra* note 46; see also BAUM AND PERRITT, *supra* note 68 at 184.

⁹³ Specific practices leading the way for acceptance of the general practice is analogous to traditional analysis in evidence law: initial close scrutiny of the trustworthiness of new technology prepares the way for future lenient acceptance of the new procedures -- coupled with a better understanding of the risks.

⁹⁴ See note 5 *supra* (providing definitions for each of these security services).

⁹⁵ Value may be defined broadly by the courts -- e.g., as "[a]ny consideration sufficient to support a simple contract." *Fowler v. Smith*, 156 N.E. 913, 914 (Ohio App. ____). Cf., U.C.C. § 1-201(44) (defining value broadly); U.C.C. § 2-714(2) ("Buyer's Damages for Breach in Regard to Accepted Goods"); and U.C.C. § 1-106 ("Remedies to Be Liberally Administered") (generally providing a subjective measure of damages; Official Comment 1 "rejects any doctrine that damages must be calculable with mathematical accuracy").

both the private⁹⁷ and public sectors⁹⁸, and may go to the heart of the debate. The challenge is to determine which transactions, other than payment orders and "purely" financial transactions merit stronger information security protection (such as cryptographic-based authentication methods) than the security utilized for low value and low risk transactions. Two competing approaches on this issue are characterized as *narrow* and *broad*.

- Narrow View Argument - Based on value, transactions which merit stronger information security are comparatively few in number. Generally, the narrow view does not provide increased

⁹⁶ This includes the development of a Model Security Baseline, *see infra* Section IIc.

⁹⁷ The National Automated Clearinghouse Association ("NACHA") does not distinguish between low and high value transactions where it "recommends that ACH [automated clearing house] processors and all ACH participants employ data security techniques in accordance with ANSI standards for authentication and key management." 1992 ACH Rules at OR xvii.

⁹⁸ Cf., "'Value' . . . will be determined on a case-by-case basis. In fact, Treasury itself moves very few funds. . . . The Treasury Directive on Electronic Funds and Securities Transfer Policy . . . makes it Treasury policy that *all* Federal EFT transactions be 'properly authenticated'. The authentication measures adopted . . . are those recommended by the American National Standards Institute (ANSI) in Standard X9.9." Treasury Directive 81-80, § 2.1. *See infra* note 99.

Query the extent to which a prudent construction of the intent of various Federal information-related statutory requirements support the use of stronger security as a function of transaction value. *E.g.*, Chief Financial Officers Act of 1990, P.L. 101-576, 104 STAT. 2,838-2,855 (Nov. 15, 1990) (in part, strengthening accountability (arguably as a security service) over financial management, including with respect to "financial information, financial data and information standards, internal controls, legislation affecting financial operations and organizations, and any other financial management matter" § 302(b)); Federal Managers' Financial Integrity Act of 1982, P.L. 97-255, 31 U.S.C. § 3512 *et seq.*; 36 C.F.R. § 1234 - Electronic Records Management (and specifically § 1234.26 "Security of Electronic Records"); The Paperwork Reduction Act, 44 U.S.C. § 3506(a) (providing that "[e]ach agency shall be responsible for carrying out its information management activities in an efficient, effective, and economical manner, and for complying with the information policies, principals, standards, and guidelines prescribed by the Director"); and, with respect to the protection of government obligations, consistent with the Comptroller General's Decisions relative to the creation of binding obligations pursuant to 31 U.S.C. § 1501.

protection for purchase orders, "merely executory contracts,"⁹⁹ contract-related business documents (excluding payment orders) and other *low value*, low risk transactions. This view argues that business knows how to take care of itself, and business practices demonstrate that non-payment-related transactions are typically not communicated in a highly secured manner.¹⁰⁰ Business has determined that the cost of strongly securing purchase orders, invoices, and the like, is not commensurate with the risk.

•Broad View Argument - Individuals supporting this position believe that the scope of transactions of a value which merit stronger information security are comparatively broad. Many purchase orders, purchase order acceptances, and other non-payment documents require stronger security protection whenever the risk of loss or error associated with such documents threatens business assets or competitive position.¹⁰¹ The value of a loss or error in a non-financial instrument may not necessarily result in as immediate a loss as with a financial instrument. However, the loss of, or litigation concerning, a non-financial instrument is nonetheless of comparable or greater value (such as where consequential damages are considered). Fiduciary duties owed by corporate management to its stock holders, include prudently protecting corporate assets -- and strong security is one prudent approach. Finally, paper-based practices demonstrate that the strength of security techniques implemented for low and medium value transactions do not vary considerably (except, *e.g.*, with respect to the use of multiple signatures for authorization), because low value transactions often are "bootstrapped" to a stronger security level.

⁹⁹ "That which is yet to be executed or performed; that which remains to be carried into operation or effect; incomplete; depending upon a future performance or event." BLACK'S LAW DICTIONARY 680 (4th ed.1968).

¹⁰⁰ Historically, cryptographic methods have (for other than national security purposes) largely only been required, or largely implemented, for financial purposes.

¹⁰¹ Some advocates of the broad view argue that even this standard is too weak. Instead, they propose that any transactions of "commercial significance" or some other more encompassing standards should be used.

A consideration of value-related issues properly includes: (i) how narrowly value should be defined;¹⁰² (ii) whether value should be limited to *financial* value; (iii) if so, how broadly should *financial* be construed; (iv) how certain must value be (*e.g.*, how liquid; when should value be measured,¹⁰³ and should the potential value of consequential damages be included);¹⁰⁴ and (v) does the definition of *sensitive information* under the Computer Security Act of 1987 necessarily broaden the scope of value for such purposes?¹⁰⁵

A value limitation is ostensibly one of the most specific and well understood criteria. For example, statutes of frauds prescribe dollar limits, such as the \$500 threshold of U.C.C. § 2-201. Another example is the Federal Acquisition Regulations ("FARs") which provide for a \$25,000 threshold¹⁰⁶ and permit telephone bids/proposals or orders in an amount up to \$2,500.¹⁰⁷ Federal money laundering regulations require reporting if a \$10,000 daily aggregate amount is exceeded.¹⁰⁸ Specifying a baseline value has been criticized as both arbitrary and difficult to enforce; but, there are administrative rulings and interpretations that provide guidance and mitigate potential abuse of aggregate requirements.¹⁰⁹

¹⁰² Should the law focus on *clear value*, *face value*, *fair and equitable value*, *market value*, *true value*, or something else?

¹⁰³ In an action to recover chattel, "value" means value at time of trial, not at time of seizure thereof. Spear v. Auto Dealers' Discount Corporation, 278 N.Y.S. 561 ().

¹⁰⁴ Compare U.C.C. § 4A-305 ("Liability for Late or Improper Execution or Failure to Execute Payment Order") and U.C.C. § 2-715 ("Buyer's Incidental and Consequential Damages").

¹⁰⁵ See *infra* note 127 (defining sensitive information).

¹⁰⁶ 48 C.F.R. § 13 (Small Purchase and other Simplified Purchase Procedures) (1992).

¹⁰⁷ FAR 14.201-6(g)1 and 15.407(e)(1). The Defense FARs Supplement, 48 C.F.R. § 208.405-2 (allowing for oral procurement ordering from federal supply contractors). Also, the General Services Administration Acquisition Regulation (GSAR) has issued a final rule to increase the threshold for use of certified invoice procedures to \$2,000 or less for construction services and \$2,500 or less for supplies or services per 48 C.F.R. § 513.7001 "Certified invoice procedure for procurement not requiring a written purchase order." 57 Fed. Reg. 26,608 (June 15, 1992).

¹⁰⁸ 31 C.F.R. § 103 (1990); 31 U.S.C. § 5315 (reports on foreign currency transactions).

¹⁰⁹ *E.g.*, Administrative Rulings, Interpreting Treasury's Currency and Foreign Transactions Regulations, Fed. Reserve Reg. Serv. 88-1 (June 22, 1988).

3. Costs of Implementation - Whether and how costs of security should impact baseline criteria are important issues to resolve. It is impossible to consider meaningfully the cost of resolving a problem until the nature of the problem and the underlying *requirements* are articulated. Premature consideration of costs may eliminate viable solutions; yet, intensive focus on cost (sometimes to the exclusion of all other factors) has been the linchpin for policy and legal reform efforts. The cost debate focuses on whether the use of cryptographic methods are a necessary component of "reasonable security procedures"¹¹⁰ and whether the costs associated with cryptography are too burdensome to require.¹¹¹

This "crypto cost debate" has two main camps. Proponents of wide-spread cryptography usage argue that (i) only cryptography can adequately protect against the threats in open systems and ubiquitous computing environments, and (ii) because the costs of cryptography will decrease with increased usage, cryptography is a viable, indispensable, and appropriate requirement. Opponents of wide-spread cryptography usage argue that (i) conventional paper-based practices are fallible and consequently computer-based practices need not be any better,¹¹² and (ii) the costs of cryptography are greater than the costs associated with protecting conventional media.¹¹³ Since this debate continues to obfuscate the rational development of policy

¹¹⁰ Although the debate is focused on cryptography, a substantial proportion of fraud is traceable to inadequate conventional controls. Superior conventional controls would largely protect against such fraud (excluding the open systems issues). In this respect, the costs associated with implementing proper management controls may dwarf the costs of cryptography.

¹¹¹ "When there is a homogeneous nationwide EFT network with standardized security techniques, it will become increasingly "cost effective" for criminal elements to develop the technology required to defraud the system, because this technology, once developed, could be applied nationwide against the cardholders of hundreds or even thousands of financial institutions." ANSI X9.9 Retail PIN Standard, § A.3. (Amer. Banker's Assn. 1982). One Federal regulator (anonymous) has urged that cryptography for electronic commerce will become legally appropriate when it is "ubiquitous, user-friendly and cheap."

¹¹² This argument may fail to account for the new and improved tools, as well as the possibilities offered by modern technologies. See *supra* ABA Resolution § (a) in Section II.b. of this paper, (encouraging appropriate legal and professional education).

¹¹³ Some proponents of the substantial use of cryptography retort by asking whether cryptography is more costly than a courier or a safe to protect an original?

and rules for computer-based media, cost issues deserve further examination.

Notwithstanding this debate, the commercial information security marketplace, and particularly the commercial cryptographic marketplace, are undergoing substantial changes which impact the accuracy of the cost analysis.¹¹⁴ There is little rigorous publicly available analysis of the costs of implementing and using cryptographic methods.¹¹⁵ A cost analysis for implementation of cryptography may include the additional costs, if any, incurred as a result of:

¹¹⁴ Although market-based arguments against implementing new or stronger security mechanisms prevail, there is evidence that market demand for security products appears to have accelerated considerably. This position is cautiously, yet optimistically, presented in light of the many "false starts" which security market pundits' reports have historically missed. A recent "survey [by BIS Strategic Decisions] of Fortune 1000 companies and other firms with more than 50 employees" in four major industries found "that the most important feature[] of an E-mail system" is *security*. ELECTRONIC MESSAGING NEWS, Vol. 4, No. 19 (Phillips Business Information, Inc., Sept. 16, 1992) at 1-2 (emphasis added). Cf., "Less than 10 percent of customers ask for security. Instead they depend on security functionality being integrated into the system, and yet the security model is changing." G. Bashr, Mgr., Sun Microsystems, Inc., remarks at the National Computer Security Conference (Baltimore, Oct. 16, 1992). The Japanese tend to adhere to such a perspective. The ubiquity of cryptography is geared to grow exponentially when its functionality is integrated into hardware and software product lines -- and this is, of course, under way.

¹¹⁵ For example, NIST plans to "[i]nvestigate the economic interests involved in the DSS." Miles Smid, "draft Response to comments on the NIST proposed digital signature standard," presented at Crypto '92 (Santa Barbara, Aug. 17, 1992) at 13. Note that the Data Encryption Standard (DES) "reflects hundreds of millions of dollars in investment," Geoffrey Turner, SRI, quoted in "Board to review U.S. policy on use of cryptography." Network World, Sept. 21, 1992 at 92.

SOURCE OF COST	APPLICABLE COST CONSIDERATIONS
<ul style="list-style-type: none"> •Crypto. software licensing •Certificate purchasing •Export filing process 	<ul style="list-style-type: none"> •License negotiation •Certificate purchase costs •Legal and technical fees for export license •Perhaps these are diminishing issues if Software Publisher's Association-type policies & agreements proliferate, and export reform continues
<ul style="list-style-type: none"> •Additional cryptographic communications overhead 	<ul style="list-style-type: none"> •Size of transactions (if transaction volume is great and the size of each such transaction is small proportionally, cost is a greater factor) •Communicating certificates/CRLs, etc. •Interoperable functional standards implementation
<ul style="list-style-type: none"> •Professional training, staffing and support¹¹⁶ 	<ul style="list-style-type: none"> •Comparatively few practitioners of the art •Considerable learning curve •Technical development nontrivial & highly variable •Problems in reaching agreement on implications of certificates •User training and servicing
<ul style="list-style-type: none"> •Additional processing¹¹⁷ and storage 	<ul style="list-style-type: none"> •CRL, certificate and message signing and verification •Host-based cycles (expensive compared to PCs) •Time sensitivity of subject data (a big factor)
<ul style="list-style-type: none"> •Key and certificate management and operation •Export "diversion in place" oversight¹¹⁸ 	<ul style="list-style-type: none"> •Liabilities of certificate issuer •Bonding and liabilities of "organizational notaries" •Issuance and revocation procedures, security and audit •Drafting and executing agreements and policies •Configuration management

TABLE 4 - SURVEY OF COSTS IN IMPLEMENTING CRYPTOGRAPHY

Another cost issue requiring resolution is whether governments will develop, or make agreements with providers to supply cryptographic

¹¹⁶ One example is the training requirements under the Computer Security Act at 1987 Fed. Reg. 26,940 (June 12, 1991).

¹¹⁷ See Ronald L. Rivest, "On NIST's Proposed Digital Signature Standard," PROCEEDINGS OF THE SECOND CPSR CRYPTOGRAPHY AND PRIVACY CONFERENCE (Washington, DC, June 1, 1992) § 4.5.5 (providing an analysis of cryptographic processing costs and notes "an approximate doubling of computer power (per dollar) every two years, and an approximate increase of a factor of 4500 after twenty-five years In the year 2017, I expect computer power will be about 5000 times cheaper than it is now.").

¹¹⁸ An example of this is the costs associated with any requirements imposed on a network, and the costs to monitor or prevent actively the export of controlled technical data from the U.S. under the Export Administration Regulations.

software to small businesses or to the disadvantaged. If so, would such software distribution be viewed as illegally "in competition" with private enterprise. Recent events associated with "enhanced" or "value-added" information service provision by the Federal Maritime Commission and other agencies highlight this point.¹¹⁹ Finally, differences between private and public policy objectives should be considered since conflicting agendas affect the choices available in designing model security baselines.¹²⁰

4. Private vs. Public - Another consideration is whether, and how, baselines in the private and public sectors should vary. For example, a private sector "business risks" model may not be necessarily applicable to public sector obligations in which public servants play a non-profit and fiduciary role to the public at large. In such an environment, there may be a more compelling basis for strong security.
5. Present vs. Future - Where costs of computing continue to decrease rapidly, where availability of computers and security mechanisms continue to increase rapidly, and where there is growing confidence that "open systems" environments will become typical, should baseline requirements be skewed towards the present or the future (assuming that any requirements necessarily cannot be totally neutral as to their placement in time)?
6. Conflicting Security Requirements - Where baseline security requirements (such as statute, regulation or agreement) conflict with a particular transaction's special security requirement(s), the special requirements should preempt baseline requirements.
7. The Party(ies) Requiring Protection or Assurances - Whether the party requiring assurances or protection (*e.g.*, against revocation or repudiation) is either the originator, the recipient or a third-party beneficiary should be considered. For example, if the originator requires specific security assurances, security requirements can arguably be less stringent than where the recipient also requires assurances. This is because the originator is in the

¹¹⁹ See generally O.M.B. Management of Federal Information Resources Proposed Revision of OMB Circular A-130. 57 Fed. Reg. (No. 83) 18,296 (Apr. 29, 1992); Tariffs and Service Contracts, Federal Maritime Commission, 57 Fed. Reg. 36,268-36,311 (Aug. 12, 1992).

¹²⁰ For example, government goals in information security are typically not geared toward profit-oriented risk taking, but rather toward the prevention of fraud or other loss. Arguably, the government should not take comparable risks since it acts as a fiduciary.

better position to control the type and extent of the security applied.¹²¹ The recipient must either accept or reject that which the originator sends. TABLE 5 presents a simplified (perhaps over-simplified) comparison of various document types, the effects of which should be reflected by the Model Security Baseline.¹²² TABLE 5 is necessarily subjective -- because the primary beneficiary of security will depend upon the particular circumstances.

TYPE OF TRANSACTION	ORIGINATOR	RECIPIENT	BOTH	3RD PARTY BENEFICIARY
Complaint	X			
Credit EFT		X		
Debit EFT	X			
Deed Will		X		X
Hazardous Waste Manifest	X			X
"I.O.U."		X		X
Notice			X	
P.O. Contract			X	
Power of Attorney			X	X

TABLE 5 - PRIMARY BENEFICIARY OF SECURITY

c. A Model Security Baseline

The following Model Security Baseline ("Baseline") is presented as one approach that contributes to the development of rules affording greater certainty for the following risk assumptions. The Baseline assumes that the transactions are largely procurement or commercial in nature, and that the anticipated electronic commerce environment may include open systems. For simplicity, the Baseline creates three classes of messages:¹²³ *Level 1*, *Level 2*, and *Level 3*, each requiring

¹²¹ Originators may (depending on the implementation) optionally include cryptographically enhanced security (e.g., digital signatures) for their own protection even where not legally required to do so. Whereas, in the absence of agreement or rule, the recipient is at the mercy of the originator.

¹²² See *infra* Section II.c. The Baseline adopts the term *message* for consistency with international standards. The term *transaction* or other descriptive term can be substituted by the user.

¹²³ These three classes of transactions are substantially consistent with the three classes of information in electronic form presented in TABLE 1 - COMPARISON OF SIGNED WRITINGS AND ELECTRONIC INFORMATION, *supra* Section II.c.

incrementally stronger security, such as the use of cryptographic methods for authentication, integrity, and confidentiality purposes.¹²⁴ Three levels are within the boundaries of workable rule-making. Where more than three classes of security are desired or required, greater granularity in the levels, or additional levels with stronger or weaker characteristics can be developed responsively. The Baseline also contemplates greater specificity in subsequently derived rules using the Baseline as a tool.¹²⁵

Both legal and computer security circles have expressed the legitimate concern that security requirements should be separated from the specific security technologies and procedures implemented.¹²⁶ Although the following Baseline may be critiqued as providing an inadequate separation, it provides comparatively general (and flexible) requirements.

¹²⁴ The Baseline is intended to help navigate through the pivotal decision (and perhaps the most difficult policy controversy) of whether or not to require the use of cryptographic-based security mechanisms. The Baseline is reprinted in Appendix 1 without footnotes and other distractions.

¹²⁵ The Baseline provides a practical interface between policies and detailed rules. For example, the Baseline provides a roadmap for enforcing a security policy, and yet, it purposefully refrains from detailing cryptographic key size, levels of passwords, algorithms, whether hardware is needed to implement cryptography and other legal and security techniques, parameters and requirements. See *supra* TABLE 3 - RELATIVE LEVELS OF ABSTRACTION.

¹²⁶ Early drafts of the ABA Resolution, *supra* note 50, expressly considered cryptographic technologies. This consideration precipitated concern within the legal community that by mentioning cryptographic technologies (i) the failure to use them would create exposure, and (ii) the rules would become antiquated prematurely. Note that the computer security community has undertaken a "post-Orange Book" migration towards the separation of requirements and techniques, or functionality and assurances.

A MODEL SECURITY BASELINE - LEVEL 1

Section 1 - *Level 1 Message Attributes*. An electronically created, communicated, or stored message of the parties shall be considered a "Level 1" message where 1.a, 1.b, 1.c and 1.d are applicable -- singularly or in any combination:

- 1.a. the message(s) does not contain highly sensitive information,¹²⁷ proprietary trade secrets, or other information requiring strong privacy protection;
- 1.b. the value¹²⁸ of the message(s) [over any [thirty (30)]¹²⁹ day period] [as established by the parties] [is not expected to exceed] [does not exceed] [five thousand dollars (\$5,000)]¹³⁰ [twenty-five thousand dollars (\$25,000)] [X dollars];

¹²⁷ The use of the Computer Security Act of 1987 as a threshold for baseline criteria raises issues (and possibly problems) because most EDI information can reasonably be considered sensitive under the Act. The Baseline seeks to accommodate sensitive information under the act -- providing incrementally stronger security in its Levels. *Sensitive* is defined in the Act as:

. . . any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (The Privacy Act), but which has not been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy. The Computer Security Act of 1987, P.L. 100-235, 100 Stat. 1724 (Jan. 8, 1988) [codified primarily in 15 U.S.C. §§ 278g-3, 278g-4 and 40 U.S.C. § 7599d].

¹²⁸ Value is intended to mean actual or fair market value. Notwithstanding this definition, legal damages, the value of a loss to society (*e.g.*, environmental pollution -- potentially intangible or difficult to ascertain), as well as issues of consequential damages should also be considered. *See infra* notes 95 and 98; *Evra Corp. v. Swiss Bank Corp.*, 673 F.2d 951 (7th Cir. 1982) (failure of bank to properly handle telex wire transfer not liable for consequential damages because it had not been placed on notice of special circumstances giving rise to them).

¹²⁹ The [bracketed] portions of text in the Baseline indicate their optional character. In fact, as a model, all provisions in the Baseline are ultimately optional.

¹³⁰ The \$5,000 is intended to be an aggregate amount. Its purpose is to prevent "splitting" large orders into multiple smaller ones. The use of a value limit on multiple transactions has proven difficult to enforce because the anticipated value/volume for a future time period

1.c.no applicable law specifies alternative security measures, or otherwise preempts the applicability of the Model Baseline for the specified message; or¹³¹

1.d. the message is not highly time sensitive.¹³²

Section 2 - *Security/Reliability*. The security implemented for Level 1 messages shall include, at a minimum:

2.a. noncryptographic identification and authentication [e.g., password-user ID];¹³³

is speculative. Inflation will render the \$5,000 less important over time. A link to a government price index, such as the consumer price index might be useful. The author acknowledges that some knowledgeable legal and technical experts believe that an aggregate amount is either unnecessary or inappropriate.

¹³¹ Additional criteria could provide that: "the business situation does not present unusual elements which tend to increase the risk above normal levels." However, determining the parameters of "normal levels" could be difficult or fruitless.

¹³² See *supra* Section II.e. TRUSTED ENTITIES AND TIME STAMPING, regarding applications requires greater proof of timeliness. E.g., in *Interactive EDI*, "[f]aster EDI is a primary requirement. This is not only a requirement on the underlying communications methods, but on all functional entities within and between the trading partners . . . response times of seconds or fractions of a second, as opposed to minutes or hours, will generally be required." RECOMMENDATION TO UN/ECE/WP.4 ON INTERACTIVE EDI WITHIN THE CONTEXT OF UN/EDIFACT, TRADE/WP.4/R.842 (July 21, 1992) at 8.

Where non-repudiable proof of receipt is not critical, or where some other responsive communication is required, functional acknowledgments may contribute adequately to a security regime and should be used. See BAUM AND PERRITT *supra* note 68 at Ch. 2 (describes the format, functionality, strengths, and weaknesses of functional acknowledgments).

¹³³ "Noncryptographic identification and authentication" requires greater specificity such as by reference to National Institute of Standards and Technology (NIST) or other authoritative guidelines. Depending upon the implementation, security should minimally be of the "C2" level where the passwords are associated with an individual. Class C2: Controlled Access Protection makes "users individually accountable for their actions through login procedures, auditing of security-relevant events, and resource isolation." DEPARTMENT OF DEFENSE TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA, DOD 5200.28-STD (Dec., 1985)(hereinafter "DoD Trusted Criteria") at 15. See the corresponding *evaluation levels* delineated in the European Commission's INFORMATION TECHNOLOGY SECURITY EVALUATION CRITERIA (ITSEC), Doc. COM(90) 314 (June 1991); the draft

2.b. recognized controls to ensure authenticity,¹³⁴ integrity,
[confidentiality,] and availability;¹³⁵ and

2.c.audit trails.¹³⁶

Federal Criteria MSFR V.1.0. (1992); and the JAPANESE COMPUTER SECURITY EVALUATION CRITERIA DRAFT 1.0 (Aug. 1992).

¹³⁴ Levels 1 and 2 of the Baseline do not accommodate full non-repudiation because of their lack of a trusted time stamp. *See supra* Section II.d. and II.e.. (concerning non-repudiation and trusted time stamps).

¹³⁵ Such controls should be comparable to recognized and appropriate criteria, *e.g.*, in the nature of certain requirements included within the Class C2 Security Policy. *See* DoD Trusted Criteria *supra* note 133 at 15. *See* the various audit and control materials cited in the notes throughout this paper for further guidance.

¹³⁶ Each entity participating in a transaction (*e.g.*, each trading partner and all intermediaries) should be required to keep an audit trail. *See generally* A GUIDE TO UNDERSTANDING AUDIT IN TRUSTED SYSTEMS, National Computer Security Center, NCSC-TG-001 Version 1 (July 28, 1987); BELDEN MENKUS and ZELLA G. RUTHBERG, CONTROL OBJECTIVES, (EDP Audit Foundation, 1990); STEVE MAR *ET. AL.*, UNDERSTANDING AND AUDITING EDI AND OPEN NETWORK CONTROLS, (Inst. of Internal Auditors and Bank Admin. Inst., 1991); and OMB A-123, A-129, A-130. *See* § 13(b) Securities and Exchange Act of 1934 as amended by the Foreign Corrupt Practices Act ¶ (b)(2) of § 13; 15 U.S.C. § 78m; and FCPA as amended by the Omnibus Trade and Competition Act of 1988, PL 100-418 § 5002. The Information Security Business Advisory Group to the Senior Officials Group for Information Security (SOG-IS) of the European Commission plans to prepare a report intended, in part, to define audit trail requirements. Task S02 - User requirements for secure I.I. Systems (publication expected early 1994).

Given the reality that every computer system can be compromised from within, and that many systems can also be compromised if surreptitious access can be gained, accountability is a vital last resort . . . all significant events should be recorded and the recording mechanisms should be nonsubvertible. Auditing services support these policies. Usually they are closely tied to authentication and authorization, so that every authentication is recorded, as is every attempted access, whether authorized or not. NRC, *id.* at 88.

An audit trail will not, however, necessarily respond adequately to situations with interactions of mutually suspicious systems, such as is typified by some forms of electronic commerce.

Section 3 - *Legal Effect*. For all legal purposes, all Level 1 messages which are communicated pursuant to Section 2 shall be presumed [conclusively?¹³⁷] to be "in writing," "signed,"¹³⁸ authentic, and enforceable to no less an extent than if such messages had been undertaken using conventional (paper-based) mechanisms.¹³⁹

Level 2 and 3 messages require stronger security. The following Baseline affords Level 2 messages greater security. Enhancement of Level 1 requirements is achieved through the addition of the use of cryptographic methods for MACs or digital signatures, and optionally for stronger confidentiality protection. Additions and deletions to Baseline Level 1 messages are noted accordingly.

A MODEL SECURITY BASELINE - LEVEL 2

Section 1 - *Level 2 Message Attributes*. An electronically created, communicated, or stored message(s) of the parties shall be considered a "Level 2" message where 1.a, 1.b, 1.c and 1.d are applicable -- singularly or in any combination:

- 1.a. the message ^ contains highly sensitive information, proprietary trade secrets, or other information requiring strong privacy protection;
- 1.b. the value of the message(s) [over any [thirty (30)] day period] [as established by the parties] [is ^ expected to exceed] [^ exceeds] [five

¹³⁷ Issues associated with conclusive presumptions are discussed in Section IV. *infra* BURDEN OF PROOF AND PRESUMPTIONS.

¹³⁸ Where the message's originator intended the message to be signed and properly communicated, otherwise the presumption shall be that the transaction was intended to be in writing but not signed. A careful review of the purpose of each particular signature requirement must be undertaken; and the parties should be confident that the particular purpose of the signature requirement is met by the substituted electronic mechanisms. See *supra* TABLE 1, TABLE 2 and note 62 (proving additional signature-related issues).

¹³⁹ See BAUM AND PERRITT, *supra* note 68 at 185-186. Under the proposed Baseline, users could implement varying procedures, but if their security procedures are weaker than the Baseline's requirements, their transactions would not be assured enforceability to the extent of comparable paper-based transactions. Thus, such users would proceed at their own risk. However, see the alternative approach presented in Table 6, *infra* at Section IV. BURDEN OF PROOF AND PRESUMPTIONS.

thousand dollars (\$5,000)] [twenty-five thousand dollars (\$25,000)] [X dollars];

1.c.^ applicable law specifies alternative security measures, or otherwise preempts the applicability of the Model Baseline for the specified message; or

1.d. the message is not highly time sensitive.

Section 2 - *Security/Reliability*. The security implemented for Level 2 messages shall include, at a minimum:

2.a. noncryptographic identification and authentication [*e.g.*, password-user ID];

2.b. recognized controls to ensure authenticity, integrity, [confidentiality,] and availability;

2.c.audit trails; and

2.d. [message authentication codes (MACs)¹⁴⁰], [digital signatures] [and/or encryption for confidentiality].¹⁴¹

Section 3 - *Legal Effect*. For all legal purposes, all Level 2 Baseline messages which are communicated pursuant to Section 2 shall be presumed [conclusively?] to be "in writing," "signed," authentic and enforceable to no less an extent than if such messages had been undertaken using conventional (paper-based) mechanisms.

The following Level 3 messages have attributes which require "trusted third party" security services. Additions and deletions to Level 2 are noted. The

¹⁴⁰ This may involve using secret key techniques such as DES (*see* FIPS-PUB 46-1). *See* FIPS-PUB 113 on MACs.

¹⁴¹ This may be accomplished through the use of public key-based or conventional key-based key management and key exchange mechanism to transmit/create secret session keys for privacy of messages.

satisfaction of other legal requirements, such as negotiability, will require alternative security services.¹⁴²

¹⁴² A trusted record keeper is anticipated to be necessary to accommodate computer-based negotiable documents. See BAUM AND PERRITT *supra* note 68 at § 5.11 "-Documentary Transfers," and § 11.9 "-Negotiability and Bills of Lading" (addressing trusted record keeping mechanisms for negotiable documents); TABLE 1 - COMPARISON OF SIGNED WRITINGS AND ELECTRONIC INFORMATION, *supra* at Section II.c.

A MODEL SECURITY BASELINE - LEVEL 3

Section 1 - *Level 3 Message Attributes.* An electronically created, communicated, or stored message(s) of the parties shall be considered a "Level 3" message where 1.a, 1.b, 1.c, 1.d and 1.e are applicable -- singularly or in any combination:

- 1.a. the message ^ contains highly sensitive information, proprietary trade secrets, or other information requiring strong privacy protection;
- 1.b. the value of the message(s) [over any [thirty (30)] day period[[as established by the parties] [is ^ expected to exceed] [^ exceeds] [five thousand dollars (\$5,000)] [twenty-five thousand dollars (\$25,000)] [X dollars];
- 1.c. ^ applicable law specifies alternative security measures, or otherwise preempts the applicability of the Model Baseline for the specified message;
- 1.d. the message is ^ highly time sensitive; or
- 1.e.an acknowledgment by a notary public, or comparable "stronger" proofs or certifications is required.

Section 2 - *Security/Reliability.* The security implemented for Level 3 messages shall include, at a minimum:

- 2.a. noncryptographic identification and authentication [*e.g.*, password-user ID];
- 2.b. recognized controls to ensure authenticity, integrity, [confidentiality,] and availability;
- 2.c.audit trails;
- 2.d. [message authentication codes (MACs)], [digital signatures] [and/or encryption for confidentiality]; and

2.e.electronic notarization (time stamping and [MAC¹⁴³] [digital signature])
by a trusted entity.

Section 3 - *Legal Effect*. For all legal purposes, all Level 3 Baseline messages which are communicated pursuant to Section 2 shall be presumed [conclusively?] to be "in writing," "signed," authentic and enforceable to no less an extent than if such messages had been undertaken using conventional (paper-based) mechanisms.

As presented, Section 3 - *Legal Effect* (of all three Baseline levels) focuses on assuring that computer-based messages are afforded comparable legal effect to paper-based messages. However, because Baseline Levels 2 and 3 use incrementally stronger security mechanisms (than in Level 1) that provide greater assurances of trustworthiness, there is a compelling basis for providing other beneficial legal effects within Section 3 - *Legal Effect*. Consequently, as an alternative, Baseline legal effects should provide incrementally stronger legal presumptions and burden allocations. For example, where a party used a digital signature, the authenticity and integrity of the computer-based information should be more difficult to attack legally (or rebut) than if weaker security had been applied to the message. The following two sections consider these issues in more detail and present such a proposal.

IV. BURDEN OF PROOF AND PRESUMPTIONS

*There is no satisfactory test for allocating the burden
of proof in . . . any given issue.* ¹⁴⁴

Scant attention has been paid to burden of proof and presumption issues in electronic commerce. This is unfortunate since, after all, proof issues are at the heart of the meaningful resolution of disputes. Burden of proof and presumption

¹⁴³ There is not yet a viable infrastructure to support symmetric-based key management where several hundred thousand parties utilize a security mechanism. Also, notarization using MACing with symmetric key technology requires that verification of notarization must be provided exclusively by the notary since keys in such an implementation cannot be shared.

¹⁴⁴ GEOFFREY C. HAZARD, JR., CIVIL PROCEDURE, 322 (3rd ed. 1985) [hereinafter, "HAZARD"].

issues have been approached largely without meaningful consideration of the *dynamic* proof sets¹⁴⁵ necessary to accommodate transaction-oriented environments. Dynamic proof sets differ sharply from the relatively *static* proof sets developed for record-oriented environments. While undeniably a daunting task, and an issue worthy of further study, burdens of proof and presumptions must be examined and integrated into a workable legal framework for electronic commerce.¹⁴⁶

The development of electronic commerce rules are intimately affected by burden of proof requirements which consist of both the *risk of nonpersuasion* and the *duty of producing evidence*.¹⁴⁷ Burden of proof issues affect (i) electronic message reliability and genuineness, and (ii) admissibility and enforceability¹⁴⁸ of information in electronic form (*e.g.*, substituted for paper-based documentation).

In developing and evaluating rules governing electronic commerce, one must recognize that "[t]he burden of pleading [should be] allocated on the basis of pragmatic considerations of fairness, convenience, and policy, rather than on any general principle of pleading."¹⁴⁹ Yet, in many respects, the law's approach to the rules governing proof of facts at trial, as exemplified by the U.C.C., has been critiqued as:

remarkably casual, indeed almost haphazard. There are no general provisions constructing the evidentiary relationships of the parties, and the UCC's specific rules are insufficient to provide guidance on a host of significant and recurring problems. Predictably, the result has

¹⁴⁵ Telephone interview with Gregory P. Joseph, Esq., (Oct. 10, 1992).

¹⁴⁶ For example, maritime law is rich in presumptions because there are often no witnesses to events on the high seas. Furthermore, cargo is, as a matter of course, passed through many hands internationally. Acts such as the Carriage of Goods by Seas Act are useful for comparative purposes.

¹⁴⁷ See HAZARD *supra* note 144 at 314. U.C.C. § 1-201(8) states that the *Burden of establishing* "a fact means the burden of persuading the triers of fact that the existence of the fact is more probable than its non-existence."

¹⁴⁸ Electronic commerce legal commentators have often focused either on "enforceability" or on "evidentiary value." Query whether presumptions are the critical link between these approaches/viewpoints?

¹⁴⁹ HAZARD, *supra* note 144 at 323.

been that the goals of consistency and clarity in commercial law have not been achieved in the important area of evidentiary proof rules.¹⁵⁰

One rule allocates the burden of proof to the party having the readier access to knowledge about the fact in question.¹⁵¹ In electronic commerce, this party may vary considerably depending on the computer involved, communications architecture, applications, and the party intended to benefit from the electronic message, among other considerations.

The Federal Rules of Evidence delineate presumptions.¹⁵² Presumptions are "occasionally used to refer to the logical inference of one fact from the existence of another."¹⁵³ For example, "[i]f Smith mails at a postbox a letter to Jones, with proper address and postage on the envelope, the trier may infer that Jones received the letter."¹⁵⁴ Similarly, "[i]t has been declared that there is a presumption, not conclusive, of prompt delivery of a letter mailed in the absence of evidence to the contrary."¹⁵⁵ "The degree of persuasion required is also sometimes manipulated as a handicap against disfavored contentions. Thus if a claim is presented that a written contract was orally modified, the party claiming

¹⁵⁰ Ronald J. Allen and Robert A. Hillman, *Evidentiary Problems in - and Solutions for - The Uniform Commercial Code*, 1984 Duke L. J. 92, 93.

¹⁵¹ HAZARD, *supra* note 144 at 324.

¹⁵² "In all civil actions and proceedings not otherwise provided for by Act of Congress or by these rules, a presumption imposes on the party against whom it is directed the burden of going forward with evidence to rebut or meet the presumption, but does not shift to such party the burden of proof in the sense of the risk of nonpersuasion, which remains throughout the trial upon the party on whom it was originally cast." FED. R. EVID. 301 "PRESUMPTIONS IN GENERAL IN CIVIL ACTIONS AND PROCEEDINGS."

"Presumption" or "presumed" means that the trier of fact must find the existence of the fact presumed unless and until evidence is introduced which could support a finding of its non-existence." U.C.C § 1-201(31).

¹⁵³ 9 WIGMORE *supra* note 54 at § 2492; See *F.A.R. Liquidation Corp. v. Brownell*, 140 F.Supp. 535 (D.DE 1956) (permitting inference based on fact established by direct or circumstantial evidence of time telegram communicated).

¹⁵⁴ HAZARD, *supra* note 144 at 326.

¹⁵⁵ *Franklin Life Ins. Co. v. Brantley*, 165 So. 834 (AL 1936); see *Kiker v. Commissioner of Internal Revenue*, 218 F.2d 389, 393 (4th Cir. 1955) (there was no presumption that a letter was delivered in the ordinary course of the mails where address was not proper).

the modification must in some jurisdictions prove its contention by clear and convincing evidence."¹⁵⁶

"What, then, are the bases upon which courts or legislatures will create presumptions? For the most part they are the same kinds of reasons that influence the allocation of the production burden generally, and these may be summed up as reasons of convenience, fairness, and policy."¹⁵⁷ Additionally, distinctions in constitutional and procedural requirements for burdens of proof and presumptions in civil versus criminal proceedings must be considered.¹⁵⁸

The use of presumptions affecting validity or enforceability of information in electronic form are widespread in EDI agreements. One example is the Model Electronic Payments Agreement and Commentary ("Model Agreement"), which states that "[t]he receipt by the sender of an acknowledgment from the recipient shall constitute *conclusive evidence* that the subject communication was received and is syntactically correct."¹⁵⁹ The practical effect of a conclusive presumption¹⁶⁰

¹⁵⁶ HAZARD, *supra* note 144 at 325

¹⁵⁷ HAZARD, *id.* at 328.

¹⁵⁸ *E.g.*, Hazard notes "an intermediate test which is occasionally applied in civil controversies" -- "clear and convincing evidence." See Notes of Advisory Committee of the 1972 Proposed Rules, FED. R. CIV. P. 301. See also *infra* Table 6. Also, the way presumptions are affected by the form of action deserve consideration. Similarly, where a statute or regulation imposes criminal penalties, the affected burdens and presumptions require special consideration. Arguably, the distinction between criminal and civil presumptions should not vary where the issue is the existence or content of an information transfer, as compared to substantive matters of criminal intent. *Cf.* the following electronic commerce law which includes substantial criminal penalties:

"Any person who . . . alters or otherwise makes illegal use of trade information compiled in the data base or the electronic documents recorded in the computer files of a designated contractor, trader, trade-related institutions or agencies, shall be subject to a penalty of at least 1 year but less than 10 years imprisonment, or a maximum fine of ₩ 100,000,000." Art. 25 (Penalty). ACT ON PROMOTION OF TRADE BUSINESS AUTOMATION (LAW NO. 4479, enacted DEC. 31, 1991), reprinted in UN/ECE/TRADE/WP.4/R.872 (Aug. 4, 1992).

See generally GREGORY P. JOSEPH, MODERN VISUAL EVIDENCE, (Law Journal Seminars-Press, 1992) at §§ 7.1 thru 7.06 (provides a detailed review of the law governing computer generated evidence).

¹⁵⁹ MODEL AGREEMENT, *supra* note 46 at Section 6.3, and MODEL EDI TRADING PARTNER AGREEMENT *supra* note 14 at § 2.2., Comment 7. Query whether the expressed conclusiveness of a presumption assures that subsequent reliance on, *e.g.*, a functional

is to excuse the sender from proving receipt where the proof is entirely in the recipient's control, perhaps to do otherwise would render EDI commercially ineffective.¹⁶¹

To what extent should *conclusive presumptions* be subject to attack?¹⁶² How much evidence should be required to disprove or shift a presumption? By analogy, take the case of the mails. "If, for example, the addressee of a properly mailed letter testifies that he or she never received it, that testimony would, if believed, justify a finding of nonreceipt." "[T]he destruction of the presumption would not, however, compel a finding of non-receipt because a properly addressed letter is so likely to reach its destination that a rational inference may be drawn that it did so."¹⁶³ Should such a presumption hold in electronic commerce matters? And, to what extent should or must there be a *rational connection* between the fact presumed and the fact proved? To illustrate the approaches taken in many domestic and international model electronic commerce agreements, the Commentary to the Model Electronic Payments Agreement presents the following addition presumptions:

Validity and Enforceability. Neither party shall contest the validity or enforceability of Transaction Sets or notices communicated pursuant

acknowledgment is reasonable, particularly in light of the recognized fallibilities of noncryptographically enhanced acknowledgments. *See supra* note 132 (discussing functional acknowledgments).

¹⁶⁰ "The *conclusive presumption* is not really a procedural device at all. Rather it is a process of concealing by fiction a change in the substantive law. When the law conclusively presumes the presence of B from A, this means that the substantive law no longer requires the existence of B in cases where A is present, although it hesitates as yet to say so forthrightly. (emphasis added). 9 WIGMORE *supra* note 54 at § 2492; and Gordon and Tenenbaum, "Conclusive Presumption Analysis: The Principal of Individual Opportunity," 71 NW. U. L. REV. 579 (1976).

¹⁶¹ However, the parole evidence rule does permit the voluntary adoption of a "super parole evidence rule" that prevents the parties from using evidence of future oral modifications. *See* U.C.C. § 2-202 "Final Written Expression: Parol or Extrinsic Evidence."

¹⁶² By definition, *conclusive presumptions* are irrefutable, yet in practice, they are sometimes refutable.

¹⁶³ HAZARD. at 330; 9 WIGMORE, *supra* note 54 at § 2489. Given the various documented instances where mail is destroyed or delayed, this presumption is suspect. Also, given that the U.S.P.S. offers multiple classes of delivery (e.g. first class, certified and registered), perhaps the presumption should be limited.

to this Agreement on grounds related to the absence of paper-based writings, signings or originals.

Each Transaction Set and notice communicated in electronic form pursuant to this Agreement shall be considered to be:

- (a) "in writing" and "written" to an extent no less than if in paper form;
- (b) "signed" where the signer includes data intended as a signature [as agreed among the parties] to an extent no less than if conventionally undertaken with pen and paper; and
- (c) an original.¹⁶⁴

Examples of other instructive presumptions include the following:

- i. If EDI messages are transmitted in accordance with an authentication procedure such as a digital signature, they shall have, between parties, a comparable evidentiary value to that accorded to a signed written document.¹⁶⁵
- ii. In an action with respect to an instrument, the authenticity of, and authority to make, each signature on the instrument is admitted unless specifically denied in the pleading. If the validity of a signature is denied in the pleadings, the burden of establishing validity is on the person claiming validity, but the signature is presumed to be authentic and authorized unless the action is to enforce the liability of the purported signer and the signer is dead or incompetent at the time of the trial of the issue of validity of the signature.¹⁶⁶

¹⁶⁴ MODEL AGREEMENT, *supra* note 46 at § 6, Comment 13.

¹⁶⁵ TEDIS, EUROPEAN MODEL EDI AGREEMENT, ART. 10 (Final Draft, 1991).

¹⁶⁶ U.C.C. § 3-308(a) ("Proof of Signatures and Status as Holder in Due Course.") "The presumption rests upon the fact that in ordinary experience forged or unauthorized signatures are very uncommon, and normally any evidence is within the control of, or more accessible to, the defendant." *Id.* Official Comment 1.

iii. If there is a discrepancy between the terms of the payment order transmitted to the system and the terms of the payment order transmitted by the system to the bank, the terms of the payment order of the sender are those transmitted by the system.¹⁶⁷

iv. A document in due form purporting to be a bill of lading . . . or any other document authorized or required by the contract to be issued by a third party shall be prima facie evidence of its own authenticity and genuineness and of the facts stated in the document by the third party.¹⁶⁸

The Model Security Baseline¹⁶⁹ includes presumptions which may vary, and which deserve further scrutiny. One immediate issue is whether the Baseline (as well as the various EDI-related model agreements) should delve further into burdens of proof and other evidentiary matters. If incrementally greater security mechanisms are used (such as in Model Baseline Levels 2 and 3), *why should not the parties receive incrementally increased presumptions as to the admissibility, credibility and weight to be afforded such messages?*¹⁷⁰ For example, TABLE 6 proposes replacing (alternatively, adding to) the Model Baseline's Section 3 - *Legal Effect* with the following presumptions for certain classes of messages. This is intended to provide a more dynamic risk-based model, and provide stronger security users with appropriate and commensurate benefits.¹⁷¹

¹⁶⁷ U.C.C. § 4A-206 ("Transmission of Payment Order through Funds-Transfer or Other Communications System.")

¹⁶⁸ U.C.C. § 1-202 ("Prima Facie Evidence by Third Party Documents.")

¹⁶⁹ Section III.c., *supra*.

¹⁷⁰ There is strong basis in the law for providing greater legal effect to documents which have been more strongly authenticated or secured; this is the case with self-proving wills and some statutes of limitations. For example, Massachusetts provides a 20 year limitation of personal actions where contracts are under seal (excluding contracts under the U.C.C.) and in actions upon promissory notes signed in the presence of an attesting witness. Otherwise, Massachusetts law provides for a 6 year limitation period on contract actions. MASS. GEN. LAWS ANN. ch. 260 §§ 1, 2 (West 1992). See Kingston Hous. Auth. v. Sandonati and Bogue, Inc., 577 N.E.2d 1, 31 (Mass. App. Ct. 1991).

¹⁷¹ It has been comically suggested that "as you move much beyond three to four levels of burdens of proof, no one except Judge Wapner could possibly understand and effectively use it." Interview with Alfred I. Maleson, Prof. Emeritus, Suffolk Univ. Law School, in Boston (Nov. 4, 1992).

MODEL BASELINE SECTION 3, LEVEL:	PRESUMPTION	(SUBSTITUTE SECTION 3 - LEGAL EFFECT)
1	Rebuttable Presumption A	Shifts burden of proof to rebut presumption by a <i>preponderance of the evidence</i>
2	Rebuttable Presumption B	Requires <i>clear and convincing</i> proof to rebut presumption of authenticity
2A (alternative to 2)	Rebuttable Presumption C	Requires proof <i>beyond a reasonable doubt</i> to rebut presumption of authenticity
3	Irrebuttable Presumption	Presumption is conclusive regardless of the opponent's evidence

TABLE 6 - SUBSTITUTE MODEL BASELINE SECTION 3 - LEGAL EFFECT¹⁷²

TABLE 6 may be preferable to the Baseline's *Section 3 - Legal Effect*, because the TABLE 6 presumptions are not inherently tied to conventional paper-based technologies. Finally, the increasing strengths of the presumptions in Table 6 are more dynamic than those of the Baseline and can be used in a multidimensional scheme.¹⁷³ Consequently, TABLE 6 deserves further consideration.

¹⁷² Transactions which do not satisfy the security criteria of Baseline Level 1 could, depending upon the legal scheme, be viewed as representing *simple presumptions* which shift the burden of going forward with the evidence, but do not change the burden of proof.

¹⁷³ For example, a scheme could be developed where a Baseline Level 1 transaction uses Level 2 security and therefore responds to a stronger presumption.

V. INTEGRATING FORMALISTIC & EVIDENTIARY REQUIREMENTS

Legal requirements for information in electronic form are typically evaluated from one of two perspectives: (i) formalistic-related requirements (*e.g.*, focusing on requirements for, or the sufficiency of, substitutes for "signed writings"),¹⁷⁴ or (ii) evidentiary-related requirements (focusing on admissibility, credibility and proof issues).¹⁷⁵ Where these perspectives are either viewed in a vacuum or adopted without contemplating their interrelationship, the resulting perspective and rules are destined to be dysfunctional. Insufficient attention has been directed toward utilizing an integrated *cradle-to-grave* analysis of the total electronic commerce environment and its requirements. To aid such an analysis, FIGURE 1 presents a representative cradle-to-grave analysis of a transaction. FIGURE 1 segments electronic commerce transactions into four phases of legal import: Phase 1-Creation (includes processing), Phase 2-Communication, Phase 3-Verification (includes retention functions)¹⁷⁶ and Phase 4-Dispute Resolution¹⁷⁷

¹⁷⁴ See Section II.a. "Treatment in the Law" *supra*.

¹⁷⁵ See Section IV. "BURDEN OF PROOF AND PRESUMPTIONS," *supra*, and notes 11-15, *supra* (concerning signature and evidentiary foundation issues, respectively).

¹⁷⁶ Transaction record storage would logically follow Phase 1 - verification -- and verification might be undertaken following each use of the stored information.

¹⁷⁷ In this hypothetical transaction: **[Phase 1]** a user creates information in electronic form to which some signature or authentication mechanism is used to satisfy legal requirements and to mitigate security threats. Then, optionally, the document is witnessed or cosigned or both, and if necessary, notarized (perhaps via a trusted crypto. box). **[Phase 2]** Next, the document is communicated to the intended recipient via third party service provider. The recipient then accesses and obtains the message. **[Phase 3]** The recipient then verifies the message for assurances of authenticity using one or more of a variety of verification techniques. Following verification, the recipient optionally can communicate an acknowledgment back to the originator such as a functional acknowledgment to notify the originator that the message was received and syntactically correct. Also, where the transaction is contractual in nature, the recipient can communicate an acceptance. **[Phase 4]** Should a dispute ensue, the parties present admissible evidence to the dispute resolution mechanism and seek to persuade the fact finder, in part, by the weight and credibility of the evidence. A decision by the fact finder completes the hypothetical.

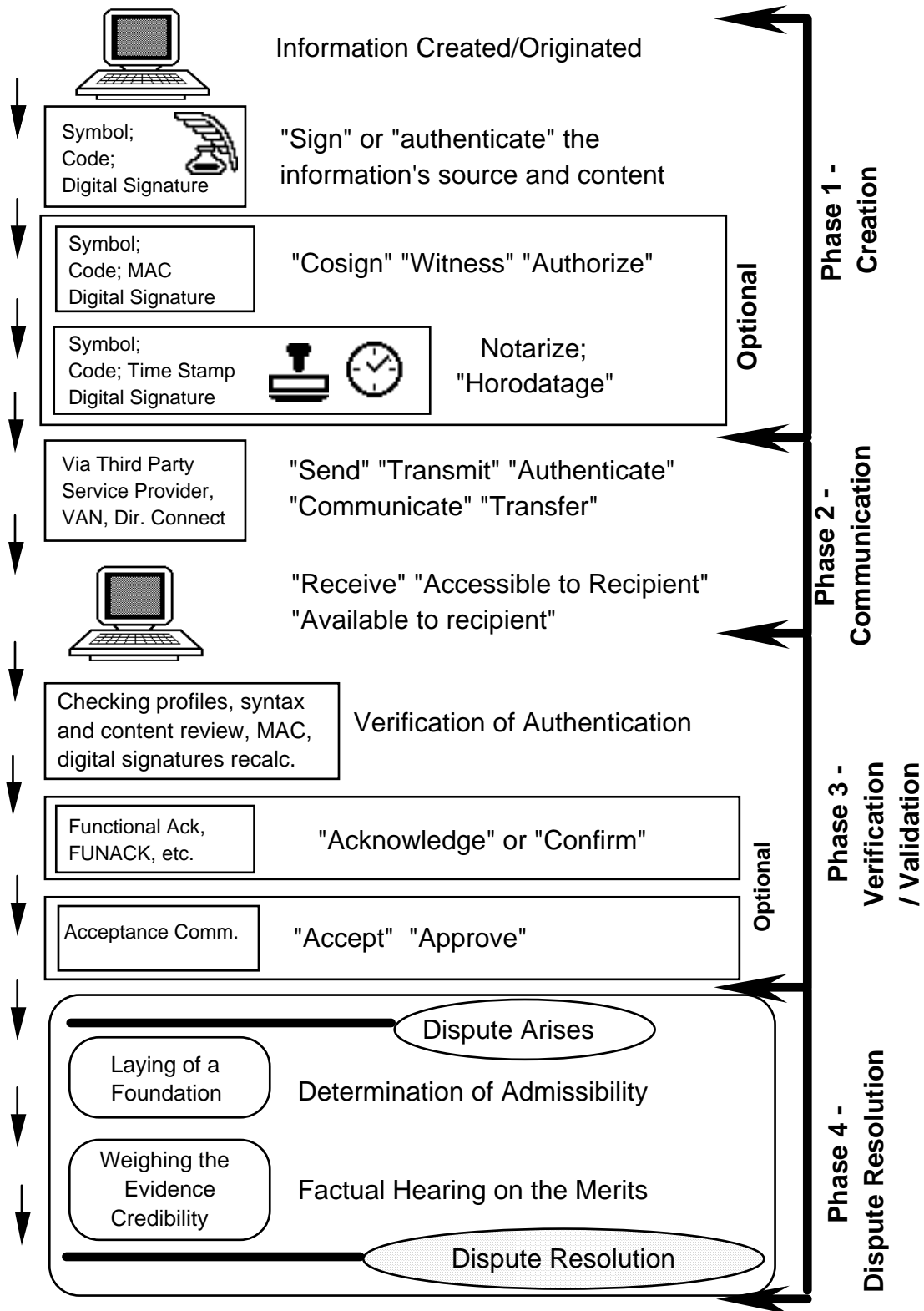


FIGURE 1 - A HYPOTHETICAL CRADLE-TO-GRAVE TRANSACTION

The remainder of this Section begins considering the following questions -- questions that deserve study beyond this paper:

- a. If formalistic requirements are reduced or eliminated¹⁷⁸ (*e.g.*, at Phase 1, FIGURE 1), will the evidentiary requirements of laying a foundation (preliminary evaluation of authenticity and relevancy) necessarily shift to a factual determination of weight and credibility?¹⁷⁹
- b. If so, will such a shift either increase or decrease the total quantum of proof required (*e.g.*, at Phase 4, FIGURE 1) from either party. Further, will it qualitatively shift the *status quo* to the unintended or unjustified disadvantage of one of the parties?
- c. Should the evidentiary requirements for laying a foundation be minimized, thereby further rendering the litigation to one of credibility and weight of the evidence?

If both formalistic and evidentiary foundational requirements are minimized, it is likely that a new risk will be created because the total required quantum of proof (weight and credibility) may increase. The party seeking to introduce a document cannot pre-gauge the extent of the required proof. The party cannot therefore rely on otherwise existing relatively static proof requirements. Absent definable and widely recognized formalistic requirements for electronic commerce, the current formalistic requirements for paper-based documents become less predictable. Theoretically, the potential evidentiary requirements,

¹⁷⁸ For example, these include requirements for a signatures, or their electronic analogs for the creation of enforceable documents in electronic form. If requirements for a signature are replaced by requirements for an electronic analog, then, the formalistic requirements remain, however, they simply take on a new form -- an electronic form.

¹⁷⁹ The elimination of formalistic requirements is not out of step with modern legal developments. "What is valued is not form for form's sake, but useful form." LAWRENCE M. FRIEDMAN, *A HISTORY OF AMERICAN LAW* 278 (Touchstone Book, 2nd ed. 1965) "The statute of frauds survived; other formalities, which had no useful place, disappeared from the law of contract." "In general, sentiment and tradition had little place in commercial law; what survived was the fit and the functional." *Id.* at 279. It is precisely the signature, of course, which is alleged by many contemporary scholars and practitioners to be formalistic, unfit and dysfunctional.

Similarly, "[t]he advantage of the writing was not only that it furnished better proof. . . but also that it made it possible to enforce obligations for which there would otherwise have been no proof at all." OLIVER WENDELL HOLMES, *THE COMMON LAW* 262 (1881).

including the burden of proving transactions, become infinite. TABLE 7, presents some of the proffered relationships between formalistic, evidentiary foundational, and proof requirements.¹⁸⁰

STATUTE OF FRAUDS OR COMPARABLE FORMALISTIC REQUIREMENTS		RELATIVE STRICTNESS OF REQUIREMENTS OF LAYING A FOUNDATION FOR ADMISSIBILITY		ANTICIPATED EFFECT ON THE QUANTUM OF PROOF (WEIGHT & CREDIBILITY) TO ENSURE ENFORCEABILITY
Yes	+	Greater	=	Lesser
No	+	Greater	=	Medium
No	+	Lesser ¹⁸¹	=	Greater

TABLE 7 - EFFECT OF DIFFERING FORMALISTIC & FOUNDATIONAL REQUIREMENTS

Some commentators propose that all information in electronic form should be admitted into evidence.¹⁸² Under this view, the judicial process almost exclusively involves the fact finder determining the credibility of the evidence *without* the prerequisite of meaningfully laying a foundation. Alternatively, if a foundation were required, then it would be, a largely perfunctory requirement to minimize clearly irrelevant and prejudicial materials under Fed. R. Evid. 104(a) "Questions of Admissibility Generally" and Fed. R. Evid. 403 "Exclusion of Relevant Evidence on Grounds of Prejudice, Confusion, or Waste of Time", respectively. Consequently, the inquiry into reliability and trustworthiness would no longer be bifurcated into (i) laying a foundation as a prerequisite to

¹⁸⁰ Perhaps the most tenuous of relationships is between foundational and proof requirements. An accurate description of the relationship is difficult to draft. However, the relative effects between formalistic requirements and evidentiary requirements are better substantiated. Query the impact of the Civil Justice Expense and Delay Reduction Plans, 28 U.S.C. § 471 *et seq.* (provides, in part, for early judicial involvement in cases, including controlling the discovery process); Table 7 is based strictly on preliminary discussions with evidentiary experts and the author's perception; therefore, more research is required.

¹⁸¹ The author recognizes that judiciary is likely to always demand some evidentiary foundation oversight.

¹⁸² One commentator advocates that "for business records virtually everything should be admissible, unless it is inherently unreliable - and even then I have doubts about the wisdom of creating a rule applying to EDI that would exclude any evidence Exclusion due to inadmissibility is a drastic sanction that can deprive a party of its fundamental proofs." Letter from George F. Chandler, III, Esq. to Michael S. Baum (Sept. 10, 1992) (on file with author).

admissibility, and (ii) determining the weight and credibility of the evidence.¹⁸³ Table 7 illustrates the anticipated dynamics of the trade-offs between these differing policies. One interpretation suggests that the diminution of formalistic and foundational requirements (the elimination of Statute of Frauds-like requirements and the relaxation of evidentiary foundation requirements) may not necessarily reduce electronic commerce barriers and costs. One euphemism which characterizes this concept is that there is *no free lunch*. What one tends to gain in the "Creation Phase" of the transactions (*see* FIGURE 1), is later lost by a commensurate increase in "Proof Phase" requirements.

VI. CONCLUSION

This paper recognizes the contribution of appropriate security techniques, procedures and practices to the legal efficacy of electronic messages and records. There is an inherent linkage between security and legal efficacy that is not adequately appreciated. The security of electronic messages and records is not only a business requirement,¹⁸⁴ but also is an underlying legal requirement. Defining this linkage is indispensable to the rational and pragmatic development of reliable electronic commerce. When the law determines what is sufficiently secure, it must consider the particular message's risks and purpose(s). Legal requirements should clarify *reasonable security procedures* without sacrificing needed flexibility. It is not a question of "having security" or "not having security" rather, it is a question of the *strength* of the security mechanisms implemented. When this legal-security linkage becomes broadly recognized, then the progress in the law which the electronic commerce community deserves and demands will begin.

¹⁸³ In practice, however, the bifurcation has sometimes been blurred. "Any evidentiary shortcoming [in developing a foundation for admission of printouts from a computer retrieval system in drug prosecution] became a matter of weight to be given to the evidence rather than one of admissibility." U.S. v. Scholle, 553 F.2d 1109, 1124-25 (8th Cir.), *cert. denied*, 434 U.S. 940 (1977).

¹⁸⁴ "Clearly, security is an essential business requirement and is, therefore, at the heart of UN/EDIFACT." UN/EDIFACT Security JWG, Draft Rec. for Security (Jul. 1992).

APPENDIX - THE MODEL SECURITY BASELINE GRAPHICS

A SECURITY BASELINE - LEVEL 1

Section 1 - *Level 1 Message Attributes.* An electronically created, communicated, or stored message of the parties shall be considered a "Level 1" message where 1.a, 1.b, 1.c and 1.d are applicable -- singularly or in any combination:

- 1.a. the message(s) does not contain highly sensitive information, proprietary trade secrets, or other information requiring strong privacy protection;
- 1.b. the value of the message(s) [over any [thirty (30)] day period] [as established by the parties] [is not expected to exceed] [does not exceed] [five thousand dollars (\$5,000)] [twenty-five thousand dollars (\$25,000)] [X dollars];
- 1.c. no applicable law specifies alternative security measures, or otherwise preempts the applicability of the Model Baseline for the specified message; or
- 1.d. the message is not highly time sensitive.

Section 2 - *Security/Reliability.* The security implemented for Level 1 messages shall include, at a minimum:

- 2.a. noncryptographic identification and authentication [*e.g.*, password-user ID];
- 2.b. recognized controls to ensure authenticity, integrity, [confidentiality,] and availability; and
- 2.c. audit trails.

Section 3 - *Legal Effect.* For all legal purposes, all Level 1 messages which are communicated pursuant to Section 2 shall be presumed [conclusively?] to be "in writing," "signed," authentic, and enforceable to no less an extent than if such messages had been undertaken using conventional (paper-based) mechanisms.

A SECURITY BASELINE - LEVEL 2

Section 1 - *Level 2 Message Attributes.* An electronically created, communicated, or stored message(s) of the parties shall be considered a "Level 2" message where 1.a, 1.b, 1.c and 1.d are applicable -- singularly or in any combination:

- 1.a. the message contains highly sensitive information, proprietary trade secrets, or other information requiring strong privacy protection;
- 1.b. the value of the message(s) [over any [thirty (30)] day period] [as established by the parties] [is expected to exceed] [exceeds] [five thousand dollars (\$5,000)] [twenty-five thousand dollars (\$25,000)] [X dollars];
- 1.c. applicable law specifies alternative security measures, or otherwise preempts the applicability of the Model Baseline for the specified message; or
- 1.d. the message is not highly time sensitive.

Section 2 - *Security/Reliability.* The security implemented for Level 2 messages shall include, at a minimum:

- 2.a. noncryptographic identification and authentication [*e.g.*, password-user ID];
- 2.b. recognized controls to ensure authenticity, integrity, [confidentiality,] and availability;
- 2.c. audit trails; and
- 2.d. [message authentication codes (MACs), [digital signatures] [and/or encryption for confidentiality].

Section 3 - *Legal Effect.* For all legal purposes, all Level 2 Baseline messages which are communicated pursuant to Section 2 shall be presumed [conclusively?] to be "in writing," "signed," authentic and enforceable to no less an extent than if such messages had been undertaken using conventional (paper-based) mechanisms.

A SECURITY BASELINE - LEVEL 3

Section 1 - *Level 3 Message Attributes*. An electronically created, communicated, or stored message(s) of the parties shall be considered a "Level 3" message where 1.a, 1.b, 1.c, 1.d and 1.e are applicable -- singularly or in any combination:

- 1.a. the message contains highly sensitive information, proprietary trade secrets, or other information requiring strong privacy protection;
- 1.b. the value of the message(s) [over any [thirty (30)] day period[[as established by the parties] [is expected to exceed] [exceeds] [five thousand dollars (\$5,000)] [twenty-five thousand dollars (\$25,000)] [X dollars];
- 1.c. applicable law specifies alternative security measures, or otherwise preempts the applicability of the Model Baseline for the specified message;
- 1.d. the message is highly time sensitive, or
- 1.e. an acknowledgment by a notary public, or comparable "stronger" proofs or certifications is required.

Section 2 - *Security/Reliability*. The security implemented for Level 3 messages shall include, at a minimum:

- 2.a. noncryptographic identification and authentication [*e.g.*, password-user ID];
- 2.b. recognized controls to ensure authenticity, integrity, [confidentiality,] and availability;
- 2.c. audit trails;
- 2.d. [message authentication codes (MACs)], [digital signatures] [and/or encryption for confidentiality]; and
- 2.e. electronic notarization (time stamping and [MAC] [digital signature]) by a trusted entity.

Section 3 - *Legal Effect*. For all legal purposes, all Level 3 Baseline messages which are communicated pursuant to Section 2 shall be presumed [conclusively?] to be "in writing," "signed," authentic and enforceable to no less an extent than if such messages had been undertaken using conventional (paper-based) mechanisms.

TEMPORARY APPENDIX

**THIS IS NOT PART OF THE PAPER, RATHER, SOME DRAFT "POSITIONS"
FOR YOUR COMMENT, HEAD SHAKING, ARGUMENT, ETC.....**

Paradigms for your consideration and comment:

1. The required security regime for information in electronic form should be such that it is capable of standing on its own rather than relying on a series of prior communications (course of conduct) to support authenticity.
2. Security is required for all messages -- it is only the strength of the security that should vary. Proof of trustworthiness as well as the underpinnings of formalistic requirements demand this.
3. NIST should take notice of existing commercial practices and to the extent applicable, as expressed in the various EDI Model Agreements (to the extent that they are being adopted by industry) -- this means that baseline messages would generally not be encrypted or digitally signed (consistent with the proposed baseline).
4. NIST should undertake a study of the current and projected costs of implementing cryptographic mechanisms for government procurement and diverse filing purposes. It should examine both public and private matters.
5. NIST should study risk analysis related to electronic commerce issues.
6. The implementation of "Reasonable Security Procedures" requires greater specificity for statutory and regulatory purposes.
7. Proof of timing of messages is important and requires greater evaluation and emphasis for regulatory purposes.
8. Burden of proof and Presumptions ...
9. The influence of government action in regulating electronic commerce will effect commercial practices. Consequently, there is compelling reason to align the private and public sector actions as much as possible.